Nr 2/2013 (75)
Biblioteczka
Komputer Świat

PARTNER WYDANIA G DATA

BEZPIECZNY KOMPUTER

JAK BRONIĆ SIĘ PRZED NOWYMI ZAGROŻENIAMI

Na płycie pełna wersja na 90 dni

G Data IS 2014

KOMPLETNY PRZEWODNIK:

- Skuteczna ochrona przed wirusami i hakerami
- Jak dbać o prywatność i bezpieczeństwo w internecie
- Walka z groźnym spamem
- Zakupy i płatności bez ryzyka
- Hasła nie do złamania
- Najlepszy sposób na backup danych
- Ochrona dziecka w sieci
- Bezpieczny tablet i smartfon

KOMPUTER ŚWIAT BIBLIOTECZKA

Więcej na: www.ebook4all.pl

BEZPIECZNY KOMPUTER

NA PŁYCIE PROGRAMY:

4Sync 1.2.6.6 | BurnAware Free 6.4 | CCleaner 4.04 | Cobian Backup 11.2 | Firefox 23 | FreeFileSync Portable 5.20 | G Data IS 2014 | Gmail Notifier Pro 5.1.1 | HijackThis 2.0.4 | KeePass 2.23 PL | KŚ B@ckup | KŚ+ | LastPass 2.0.20 | Macrium Reflect Free 5.2 | Malwarebytes Anti-Malware 1.75 | MiniTool Drive Copy 5.0 | OpenDNS Updater 2.2.1 | PirateBrowser 0.6b | Poczta systemu Windows | SpiderOak 5 | Spybot 2.1 | SpyShelter 8.5.1 Personal Free | Spyware Terminator 3.0 | Synkron Portable 1.6.2 | Thunderbird 17.0.8 | Tor Browser Bundle 2.3.25-12

Więcej programów na Wirtualnej Płycie w aplikacji KŚ+ (www.ksplus.komputerswiat.pl)

Biblioteczka Komputer Świat

BEZPIECZNY KOMPUTER

JAK BRONIĆ SIĘ PRZED NOWYMI ZAGROŻENIAMI

Więcej na: www.ebook4all.pl

Paweł Gajewski

Rafał Kamiński

Mariusz Michalski

Tomasz Paczuski

Arkadiusz Świostek

Karol Żebruń

Od autorów

Każdy, kto choć raz stracił pliki lub musiał reinstalować system po ataku wirusa, wie, że kwestii związanych z bezpieczeństwem danych nie można lekceważyć. I choć hakerzy coraz rzadziej próbują niszczyć nasze dyski, to wciąż szukają nowych metod, by utrudnić nam życie, opróżnić konta bankowe czy zarobić, wykorzystując nasze komputery do rozsyłania spamu czy dystrybucji innego szkodliwego oprogramowania. A skoro coraz większa część naszego życia toczy się w internecie, na celownik biorą także naszą tożsamość i anonimowość. Usiłują zastraszyć fałszywymi alarmami o zagrożeniach i wyłudzić pieniądze za nic niewarte programy, które tylko symulują, że chronią nas przed czymkolwiek. Sięgają po coraz bardziej pomysłowe i wyrafinowane metody, łącząc ze sobą różne techniki ataków tak perfidnie, że użytkownicy często nawet nie zdają sobie sprawy z tego, że ktoś przejął kontrolę nad ich pecetem i buszuje po dysku, wysysając stopniowo wszystkie dane, na których można w jakikolwiek sposób zarobić. Dlatego tak ważna jest świadomość zagrożeń i wiedza, jak się przed nimi chronić. Przygotowując tę książkę, za cel postawiliśmy sobie dostarczenie tych informacji w przystępnej i zrozumiałej dla każdego formie.

Z kolejnych rozdziałów dowiemy się, jakie metody stosuje cybermafia, czym objawiają się poszczególne ataki, a także, jak skutecznie chronić pecet i zgromadzone na dysku dane. Wiedzę teoretyczną popartą przykładami uzupełniono o przejrzyste porady krok po kroku, dzięki którym nasz komputer będzie w stanie ochronić się przed wszelkimi szkodnikami. Znakomitym dopełnieniem książki jest płyta z 25 programami do zabezpieczeń. Na ich przykładzie dowiemy się, jak najlepiej skonfigurować ochronę komputera. Czytelnicy mogą też za darmo przez 90 dni korzystać z profesjonalnego pakietu bezpieczeństwa G Data InternetSecurity 2014 i nabyć jego pełną wersję w atrakcyjnej cenie, a także kupić z dużym rabatem program G Data MobileSecurity 2 przeznaczony do zabezpieczania smartfonów i tabletów z systemem Android.

Zapraszamy do lektury!

BEZPIECZNY KOMPUTER

Wstęp 2

Od autorów ... 2
Bezpieczeństwo przede wszystkim ... 4

1. NAJWIĘKSZE ZAGROŻENIA 6

Co zagraża naszemu pecetowi ... 7
Podstawa dobrego zabezpieczenia ... 11
Jak korzystać z pakietu G Data InternetSecurity 2014 ... 13
Dodatkowe zabezpieczenia ... 18

2. BEZPIECZNE DANE 20

Wybór miejsca na kopie zapasowe ... 21
Kopia dużych zbiorów plików ... 22
Backup w chmurze ... 24
Kopia zapasowa systemu Windows ... 27
Odświeżanie Windows 8 ... 29

3. BEZPIECZNE DZIECKO 30

Zabezpiecz komputer ... 31
Kontrola rodzicielska ... 32
Dostęp do internetu ... 34
Kontrola rodzicielska w G Data InternetSecurity 2014 ... 36

4. BEZPIECZNIE ONLINE 38

Zagrożenia w sieci ... 39
Korzystanie z usług w internecie ... 41
Publikowanie treści w internecie ... 42
Śledzenie naszych działań ... 44

5. BEZPIECZNY E-BANK 46

Bezpieczny komputer to podstawa ... 47
Podstawowe środki bezpieczeństwa ... 48
Jak rozpoznać phishing bankowy ... 49
Bezpieczne płatności internetowe ... 51
Zagrożenia związane z kartami ... 52
Zagrożenie czai się w skrzynce ... 53

6. BEZPIECZNE ZAKUPY W SIECI 54

Zanim zaczniemy zakupy ... 55
Bezpieczeństwo zakupów ... 56
Zakupy za granicą ... 59
Jak pewnie i bezpiecznie płacić ... 61

7. PRYWATNOŚĆ, ANONIMOWOŚĆ 62

Optymalne ustawienia prywatności w serwisach społecznościowych ... 63
Zamykamy swoje konta w serwisach społecznościowych ... 67
Co internet o mnie wie ... 69
Surfujemy bez śladów w komputerze ... 71
Usuwamy ślady przeglądania z komputera ... 72
Trzy sposoby na anonimowy dostęp do internetu ... 72

8. E-MAIL BEZ ZAGROŻEŃ 74

Bezpieczny komputer ... 75
Spam – walka z niechcianą pocztą ... 76
Solidne konto pocztowe z dobrym filtrem ... 77
Ochrona poczty e-mail w G Data ... 78
Szyfrowanie wiadomości e-mail ... 80
Phishing, czyli wyłudzanie danych ... 80

9. BEZPIECZNE HASŁA 82

Co to są bezpieczne hasła ... 83
Tworzymy bezpieczne hasła ... 86
Menedżery haseł ... 87

10. SMARTFON I TABLET 90

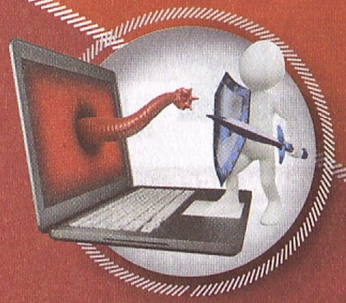
Jak zapewnić bezpieczeństwo ... 91
Korzystamy z wbudowanych funkcji ... 93
Pakiet bezpieczeństwa od G Data ... 99

DODATKI / REDAKCJA 100

Pakiet G Data IS 2014 dla Czytelników ... 100
Trudne pojęcia i terminy ... 102
Stopka redakcyjna ... 104

Więcej na: www.ebook4all.pl

BEZPIECZEŃSTWO PRZEDE WSZYSTKIM



SPAM I PHISHING

Niechciana poczta nadal zalewa nasze skrzynki. Bezpośrednio najczęściej nie niesie zagrożenia – jest tylko uciążliwa. Gorzej, gdy za pomocą spamu z phishingiem cybermafia pozyska dane naszych kont bankowych czy dane logowania do serwisów internetowych. Więcej na ten temat na stronach 74–81.

UTRATA DANYC

Brak kopii ważnych d nych może oznacza dla nas katastrof O backupie dany przeczytan na strona 20–2

RADZIEŻ SPRZĘTU

martfon czy tablet – łakome kąski dla odziei. Jak zabezeczyć przed nimi rzęt? Czytaj stronach 0–99.

TOŻSAMOŚĆ

Na celowniku cyberprzestępców znajduje się także nasza cyfrowa tożsamość. Gdy hakerzy przejmą nasze konta e-mail, profile społecznościowe, listy kontaktów i inne dane, podszywając się pod nas, mogą zniszczyć naszą opinię nie tylko w świecie wirtualnym, ale także realnym. Więcej na ten temat na stronach 38–45 i 62–73.

WIRUSY

Obecnie wirusy nie niszczą danych na zainfekowanych dyskach. Dlaczego? To proste: na tym nie daje się zarobić! Cyberprzestępcy wykorzystują wirusy, trojany, rootkity, spam i inne metody, by wykradać nasze dane, korzystać z mocy obliczeniowej zarażonego komputera czy jego dostępu do sieci. Dziś infekcja wirusem może narazić nas na sporo więcej nieprzyjemności niż utrata kilku plików czy konieczność reinstalacji systemu operacyjnego na komputerze. Więcej na ten temat przeczytamy na stronach 6–19.

ANONIMOWOŚĆ

Przekonani o własnej prywatności i anonimowości, w swoich domach korzystamy z internetu, zostawiając mnóstwo śladów i informacji o sobie. Te dane to największy skarb firm reklamowych, które bez pardonu handlują nimi, by jeszcze skuteczniej atakować nas reklamami i przewidywać, co zrobimy w bliższej lub dalszej przyszłości. Mamy prawo i obowiązek chronić swoją prywatność! Informacje, jak to zrobić skutecznie, znajdziemy na stronach 38–45 i 62–73.

CYBERPRZESTĘPCY

Jeszcze kilka lat temu wszyscy drżeliśmy w obawie przed hakerami. Obecnie haking to tylko jeden z odłamów cybermafii. A ta z kolei wykorzystuje wszystkie dostępne techniki i technologie, by czerpać spore profity: sprzedawać wykradzione numery kart kredytowych, opróżniać konta bankowe, szantażować i zastraszać użytkowników komputerów, rozsyłać spam czy blokować ważne serwisy internetowe. Więcej na temat ochrony przed internetową mafią przeczytamy na stronach 6–19.

ZAKUPY W SIECI

Nieuczciwy sprzedawca, problemy z dostawą z zagranicy, cło, podatki, reklamacje, niedozwolone zapisy w regulaminach sklepów internetowych, zwykli naciągacze... Gdy coraz więcej zakupów robimy online, kluczowe staje się, by znać swoje prawa i ścieżkę ich egzekwowania. Tylko w ten sposób uchronimy się przed nieuczciwymi handlarzami i przykrymi niespodziankami podczas zakupów dokonywanych przez internet. Więcej o zakupach w sieci na stronach 54–61.

ZAGROŻENIA MOBILNE

Smartfony i tablety zawierają nasze zdjęcia, e-maile, kontakty, dane kont bankowych i wiele innych informacji. Dlatego są pod szczególnym ostrzałem ze strony cyberprzestępców. O tym, jak zabezpieczyć komórkę i tablet, przeczytamy na stronach 90–99.

HASŁ ANKI NLINE

To samo, pros hasło do każ usługi, ban i serwisu? Kieps pomysł! Dlaczeg

kkomyślność zy płatnościach nkowych może nas ono kosztować. Więj – na stronach 46–53.

Patrz strony 82–8

DZIECKO

Najmłodsi narażeni są na szkodliwe treści w internecie lub po prostu – zbyt długie przesiadywanie przed komputerem. A jeśli pecet dzielimy z dziećmi, warto zadbać, by nie zniszczyły nam efektów pracy czy ważnych dokumentów. O ochronie dzieci przeczytamy na stronach 30–37.

Więcej na: www.ebook4all.pl

1 Największe zagrożenia

Aby skutecznie zabezpieczyć pecet przed zagrożeniami, najpierw trzeba je gruntownie poznać. Pomogą nam w tym informacje zawarte w tym rozdziale

Komputer zaczął wolniej działać? Na pulpicie pojawiają się dziwne komunikaty? Popsuł się antywirus i nie można go uruchomić? Łącze internetowe jest ciągle zapchane, choć nic nie ściągamy? W przeglądarce stron WWW otwierają się strony, z których nie korzystamy? Takie objawy mogą być efektem ataku wirusa lub innego szkodnika. Do infekcji wystarczy często jedynie otworzenie strony internetowej – nowoczesny **malware*** po kryjomu sam się pobierze i zainstaluje na dysku naszego komputera. W tym rozdziale znajdziemy informacje o rodzajach zagrożeń, porady, za pomocą jakich aplikacji się przed nimi chronić, i wskazówki, jak pozbyć się z dysku wszystkich szkodników. Poznamy najważniejsze moduły pakietu bezpieczeństwa typu Internet Security – do czego służą i jak z nich efektywnie korzystać, a także uzyskamy wiedzę, jakimi narzędziami warto tę linię obrony wzmocnić. **rk**

DROGOWSKAZ

- Co zagraża naszemu pecetowi s. 7
- Podstawa dobrego zabezpieczenia s. 11
- Jak korzystać z pakietu G Data InternetSecurity 2014 s. 13
- Dodatkowe zabezpieczenia s. 18

PRZYDATNE PROGRAMY

- G Data InternetSecurity 2014 CD-KOD: 007
- KŚ+ CD-KOD: 013
- Malwarebytes Anti-Malware CD-KOD: 016
- SiteAdvisor TYLKO W KS+
- Secunia PSI TYLKO W KS+

*Wyjaśnienie pojęcia w leksykonie na stronach 102–103

Co zagraża naszemu pecetowi

Jeszcze kilka lat temu łatwo było sklasyfikować zagrożenia atakujące nasze komputery: kilka rodzajów wirusów i ataki hakerskie. Obecnie jednak większość szkodników realizuje wiele różnych funkcji, przez co każde złośliwe oprogramowanie może należeć do kilku kategorii. Poznajmy najważniejsze z nich (kolejność alfabetyczna).

Adware

Programy typu adware uznawane są za tak zwane PUP (ang. *Potentially Unwanted Program*) – potencjalnie niechciany program. Nie niosą ze sobą większego zagrożenia, ale mogą w swoim oknie wyświetlać irytujące reklamy lub otwierać dodatkowe okna przeglądarki, w których wyświetlają się reklamy, za które twórcy adware'u dostają pieniądze.

Bomba logiczna

Może realizować dowolne szkodliwe funkcje, ale do ich aktywacji muszą wystąpić określone warunki – najczęściej data, wykonanie operacji na wybranym pliku, uruchomienie wskazanego programu czy nawiązanie połączenia z internetem.

Botnet (komputery zombie)

Zainfekowane komputery działają względnie normalnie, co jest w interesie twórców botnetu. W tle jednak włączone są ukryte funkcje i procesy, przez co nasz komputer może być bez naszej wiedzy wykorzystywany do: przeprowadzania ataków na inne systemy komputerowe, rozsyłania spamu, zacierania śladów innych ataków czy wykonywania różnych obliczeń. Twórcy botnetów czasami wprowadzają do swoich szkodników funkcje pozwalające podglądać ekran naszego peceta. Więcej o botnetach przeczytamy w ramce na stronie 9.

Hijack

Uciążliwy rodzaj ataku, który polega na podmianie strony startowej przeglądarki stron WWW i ustawień wyszukiwania. W wypadku takiego zagrożenia nasza przeglądarka otwiera nieznaną nam stronę (często upodobnioną do Google), a wyszukiwanie za pomocą paska adresu przeglądarki wyświetla nam wyniki z wyszukiwarki innej niż domyślnie ustawiona w systemie.

Keylogger

Funkcja realizowana przez keylogger jest prosta: ma zapisywać wszystko, co wpisujemy za pomocą klawiatury. Te szkodniki wykorzystywane są najczęściej do wykradania loginów i haseł, numerów kart kredytowych i kodów weryfikujących czy po prostu szpiegowania użytkowników.

Królik (lub bakteria)

Na zainfekowanym komputerze uruchamia i tworzy kolejne swoje kopie aż do zapisania całego wolnego miejsca na dysku komputera i zajęcia całej dostępnej pamięci operacyjnej peceta. W efekcie komputer działa coraz wolniej lub nawet zawiesza się.

Eksperci G Data ostrzegają!
Ponad 2,6 mln nowych zagrożeń na syste indows pojawiło się w 2012 roku.

Więcej na: www.ebook4all.pl

Phishing
Poprzez podszywanie się pod znane nam instytucje i firmy (banki, sklepy i tym podobne) hakerzy wyłudzają dane dostępowe do kont. Najczęściej phishing otrzymujemy w formie e-maila z odnośnikiem do podrobionej strony, na której znajduje się okno logowania – wprowadzone w nie dane trafiają bezpośrednio do cyberprzestępców.

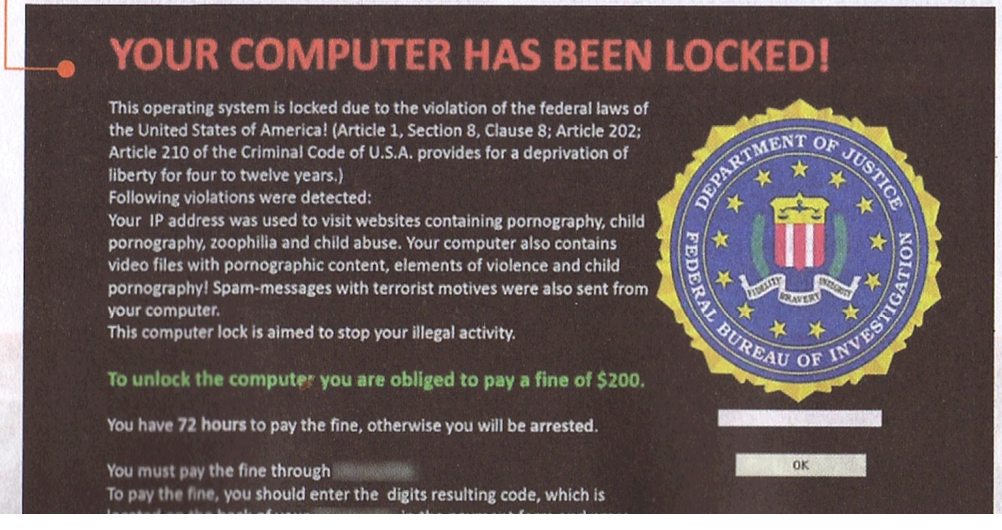
Trojan
Nazwany na cześć mitologicznego konia trojańskiego szkodnik podszywa się pod przydatne dla nas oprogramowanie, a po kryjomu instaluje dodatkowe szkodliwe funkcje i procedury.

Ransomware
Złośliwe oprogramowanie tego typu blokuje nam całkowicie dostęp do komputera i wyświetla żądanie okupu (ang. *ransom* – okup): jeśli zapłacimy cyberprzestępcom, pecet zostanie odblokowany.

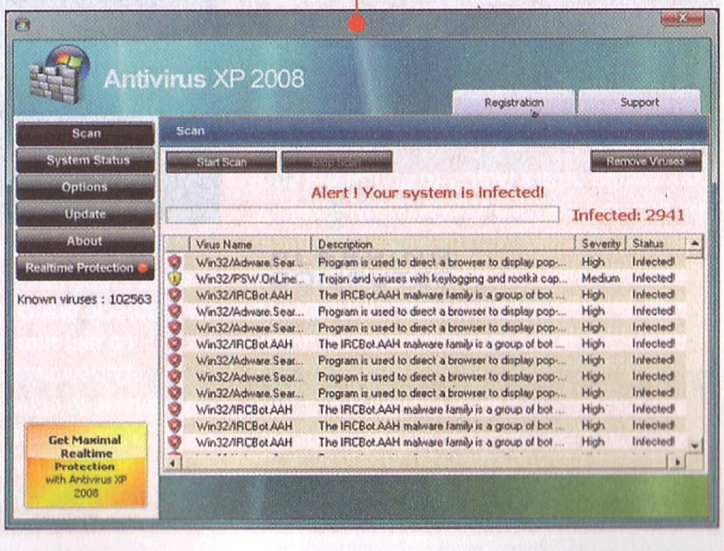
Robak
Działa podobnie jak wirus. Podstawową różnicą jest to, że do działania nie potrzebuje pliku-nosiciela. Zamiast tego wykorzystuje luki w zabezpieczeniach systemu i zainstalowanych programów, by się powielać i rozprzestrzeniać. Od twórcy robaka zależy, w jakie funkcje destrukcyjne czy szpiegowskie szkodnik zostanie wyposażony.

Rootkit
To wyjątkowo perfidny szkodnik, którego celem jest ukrycie w naszym systemie operacyjnym siebie i innych niebezpiecznych procesów tak, aby program antywirusowy nie był w stanie ich wykryć. Może realizować różne funkcje – na przykład ściągać na dysk peceta inne wirusy.

Scareware
To fałszywe programy antywirusowe. Pobieramy je często pod wpływem impulsu, gdy na zmanipulowanej stronie internetowej wyświetlają się komunikaty o infekcji w naszym komputerze lub też gdy inny szkodnik działający na naszym pececie wyświetli taki komunikat (często udający komunikat systemowy). Gdy uruchomimy scareware, zostaniemy zasypani informacjami o wykrytych szkodnikach, ale ich rzekome usunięcie będzie możliwe dopiero, gdy wykupimy pełną wersję programu. Po zapłaceniu kosztów licencji uciążliwe komunikaty znikają.



Spyware
Oprogramowanie szpiegujące, które zbiera informacje na nasz temat: adresy odwiedzanych stron, numery kart płatniczych, loginy i hasła (wykorzystując funkcję keyloggera),



MILIONY ZOMBIE
Najbardziej aktywny w pierwszej połowie 2013 roku botnet ZeroAccess swoim zasięgiem objął ponad 2 miliony komputerów na całym świecie. Zainfekowane maszyny – komputery zombie – bez wiedzy swoich właścicieli przetwarzają dane służące do zdobywania bardzo wartościowej wirtualnej waluty **Bitcoin***, na czym operatorzy botnetu mogą zarabiać miliony dolarów. Druga grupa zarażonych pecetów wykonuje bez wiedzy użytkowników operacje klikania na reklamy (tak zwana kradzież kliknięć – ang. *click fraud*), co według specjalistów od bezpieczeństwa informatycznego może przynosić cybermafii zyski w wysokości nawet 100 tysięcy dolarów dziennie. ZeroAccess nie jest jednak wcale największym botnetem. Rekordziści, jak BrediLab, ZeuS, Mariposa, Grum czy Rustock, zasięgiem obejmowali nawet kilkadziesiąt milionów zainfekowanych maszyn.

Według raportu CERT Polska w 2012 roku w Polsce najbardziej aktywne były trzy botnety: Virut (ataki DDoS, spamowanie i kradzież danych) wykryto na prawie 900 tysiącach komputerów w naszym kraju, DNSChanger (przekierowywał na podrobione strony banków i sklepów) na blisko 430 tysiącach, a ZeuS na około 250 tysiącach (przekierowywał na podrobione strony banków, zmieniał numery kont w przelewach i przechwytywał hasła jednorazowe do naszych transakcji bankowych).

* Wyjaśnienie pojęcia w leksykonie na stronach 102–103

Więcej na: www.ebook4all.pl

adresy naszych kontaktów, zrzuty ekranu.

Stealware

Gdy szkodnik tego typu wykryje próbę płatności internetowej, podmienia bez naszej wiedzy dane odbiorcy, przez co przelew lub płatność trafiają na konta internetowej mafii.

Wirus komputerowy

Najważniejszą cechą wirusa, tak jak jego odpowiednika ze świata biologicznego, jest zdolność do powielania się. Potrzebuje jednak nosiciela – podczepia swój kod do zarażonego pliku. Może mieć wbudowane różne funkcje destrukcyjne, jak na przykład kasowanie plików czy uszkadzanie systemu operacyjnego.

ATAKI NA SERWISY INTERNETOWE

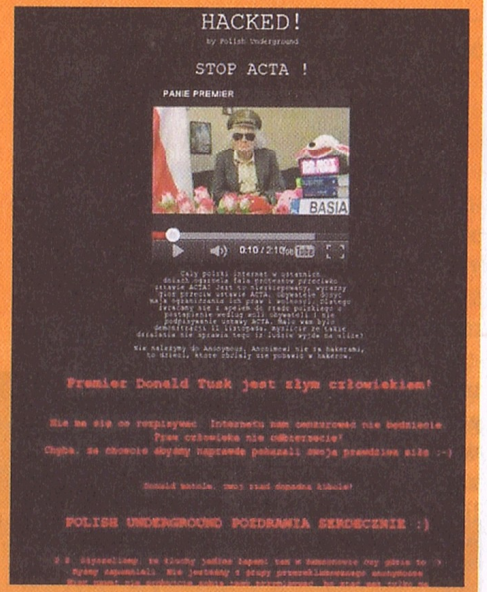
Na celowniku cyberprzestępców są nie tylko komputery domowych użytkowników. Zorganizowane grupy przestępcze często atakują także serwisy internetowe.

DDoS

Atak typu Distributed Denial of Service często wykonywane są z użyciem botnetów. Komputery-zombie godzinami ponawiają próby nawiązania połączenia ze wskazaną stroną internetową, powodując przeciążenie łącza i serwera, przez co witryna przestaje być dostępna w sieci. Z atakiem tego typu w pierwszej połowie 2013 roku zmagał się polski serwis aukcyjny Allegro.

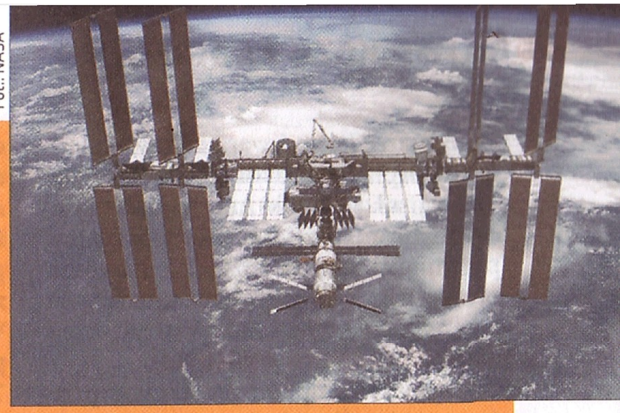
Deface

Tak zwana utrata twarzy to podmiana strony głównej serwisu WWW. Odwiedzający zamiast oficjalnej witryny widzą informacje przygotowane przez hakerów – najczęściej jakąś formę manifestu społecznego czy politycznego, czy po prostu przechwałki. Wiele ataków tego typu było przeprowadzanych w 2012 roku jako protest przeciwko próbom wprowadzenia kontrowersyjnych przepisów ograniczających wolność w internecie (ACTA).



Strona www.premier.gov.pl podmieniona przez grupę hakerów Polish Underground w proteście przeciwko ACTA. Umieszczono na niej film znanej w sieci Pani Basi stylizowany na wystąpienie generała Jaruzelskiego ogłaszającego stan wojenny. Stronę usunięto, ale sam film można obejrzeć na www.komputerswiat.pl, podając WebKod: 63872

Fot.: NASA



WIRUSY W KOSMOSIE

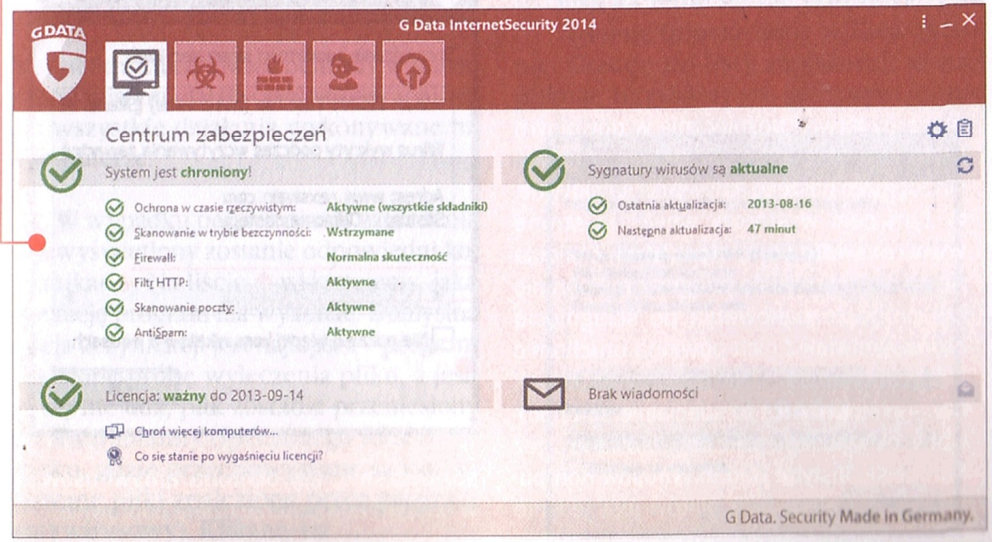
W 2008 roku na dwóch laptopach astronautów rezydujących na Międzynarodowej Stacji Kosmicznej wykryto wirus W32.Gammima.AG. Działanie szkodnika polegało na wykradaniu z komputerów danych logowania do gier internetowych, szczególnie popularnych w Chinach.

Podstawa dobrego zabezpieczenia

Poznaliśmy najczęściej występujące zagrożenia, na które narażony jest nasz komputer. Z tej części rozdziału dowiemy się natomiast, w jakie programy wyposażyć pecet, by stawić czoło szkodnikom. Główne składniki ochrony komputera poznamy na przykładzie pakietu G Data InternetSecurity 2014, z którego Czytelnicy książki mogą za darmo korzystać przez 90 dni (szczegóły na stronach 100-101).

Antywirus

Chroni przed wszelkimi szkodnikami (wirusy, spyware, dialery, rootkity, trojany), które mogą przedostać się na nasz komputer zarówno poprzez sieć, jak i pamięci USB. Wykorzystuje technologię CloseGap, która na bieżąco niweluje luki w systemie. Do skanowania w tle, jak i na żądanie wykorzystywany jest podwójny silnik skanujący, w tym mechanizm BitDefendera. Dys-



Więcej na: www.ebook4all.pl

ponuje narzędziem Kwarantanny, blokuje przed rozprzestrzenianiem się zagrożeń przez e-mail. Składniki Antywirusa zapewniają ochronę przed oszustwami on-line (phishing) i dbają o bezpieczeństwo naszych płatności w sieci (BankGuard).

Firewall (zapora ogniowa)

Zabezpiecza komputer przed cyberprzestępcami i próbami nieautoryzowanego dostępu do danych zgromadzonych na komputerze. Monitoruje połączenia sieciowe (przewodowe i bezprzewodowe) i informuje o blokowanych programach (można tworzyć własne reguły) oraz próbach ataku z zewnątrz.

Antyspam

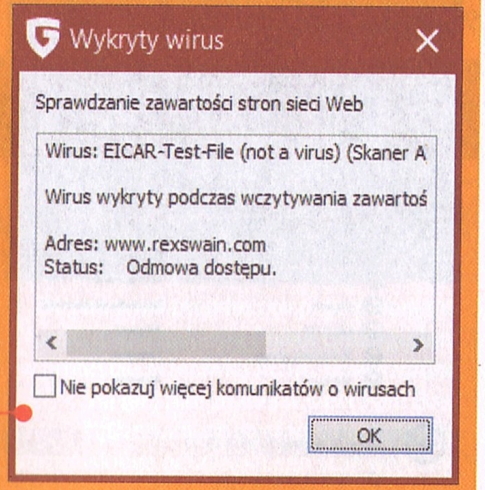
Oznacza niechcianą korespondencję jako spam na podstawie list adresów i słów kluczowych. Reguły możemy samodzielnie dostosować. Wykorzystuje także informacje z chmury internetowej, by wykryć ewentualne zagrożenia, zanim jeszcze powstaną odpowiednie szczepionki (tak zwana funkcja Spam-OutbreakShield). Więcej na temat ochrony przed spamem przeczytamy w rozdziale 8 na stronach 74-81.

Kontrola rodzicielska

Moduł, którego zadaniem jest określenie zasad i monitorowanie poczynań najmłodszych użytkowników komputera. Pozwala filtrować treści wyświetlane przez dziecko, odwiedzane strony internetowe czy określać czas, w jakim możliwe jest korzystanie z komputera. Więcej na ten temat przeczytamy w rozdziale 3 na stronach 30-37.

PRZETESTUJ SWÓJ ANTYWIRUS

Jeśli nasz program antywirusowy od dłuższego czasu nie powiadamia nas o żadnych zagrożeniach, niekoniecznie oznacza to, że jesteśmy bezpieczni. Być może jakiś szkodnik zablokował jego działanie! Na szczęście możemy łatwo i bezpiecznie w dowolnym momencie sprawdzić, czy funkcje wykrywania zagrożeń naszego antywirusa są aktywne. W tym celu wystarczy wejść na stronę **www.rexswain.com/eicar.html**. Znajdują się na niej trzy pliki do ściągnięcia. Pobranie lub próba rozpakowania po ściągnięciu któregokolwiek z nich powinna uruchomić alarm antywirusa. Nie musimy się jednak bać - pliki **EICAR*** to specjalnie spreparowane, nieszkodliwe pliki, przygotowane przez Europejski Instytut Badań Wirusów Komputerowych. Celem tych plików jest jedynie sprawdzenie, czy ochrona antywirusowa w naszym komputerze działa poprawnie.



* Wyjaśnienie pojęcia w leksykonie na stronach 102-103

Niszczarka

Kasuje pliki z danymi tak, by ich odzyskanie w jakikolwiek sposób było już niemożliwe. To niezbędne narzędzie, gdy na przykład chcemy sprzedać używany dysk twardy i obawiamy się, że wścibski kupiec może próbować odzyskać z niego nasze dane.

Menedżer autostartu

Proste w użyciu narzędzie, które pozwala określić priorytet uruchamiania się poszczególnych aplikacji podczas startu systemu. Dzięki temu ważne dla nas programy mogą być włączane wcześniej, a rzadziej używane - z opóźnieniem.

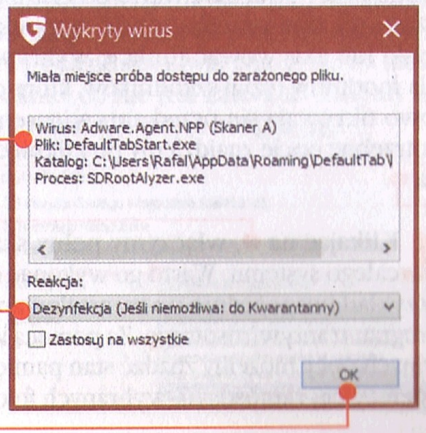
Jak korzystać z pakietu G Data InternetSecurity 2014

Zgodnie z opisem na stronach 100-101 instalujemy pakiet G Data InternetSecurity 2014. Po zakończeniu tego procesu nasz komputer jest już dobrze chroniony. Zobaczmy więc, jak używać składników bezpieczeństwa. W tym rozdziale zapoznamy się z modułem antywirusa i firewalla. Szczegółowe omówienie funkcji związanych z ochroną dzieci i poczty znajdziemy w rozdziałach 3 i 8.

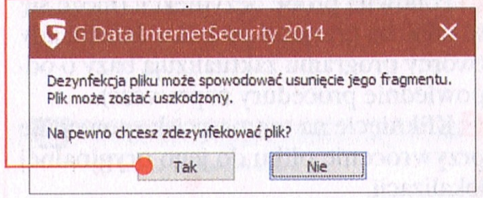
Co zrobić po wykryciu szkodnika

Moduł Strażnika, a więc ochrony w czasie rzeczywistym, działa ciągle w tle, analizując wszystkie działania wykonywane na komputerze.

1 W wypadku pojawienia się zagrożenia wyświetlony zostanie odpowiedni komunikat. Na liście wskazujemy, jaką operację program ma wykonać. Domyślna opcja dezynfekcji jest najlepsza - program podejmie próbę wyleczenia pliku, a jeśli to się nie uda, plik zostanie przeniesiony do Kwarantanny (specjalnego folderu na dysku, gdzie przechowywane są zainfekowane pliki znalezione przez program antywirusowy). Klikamy na .

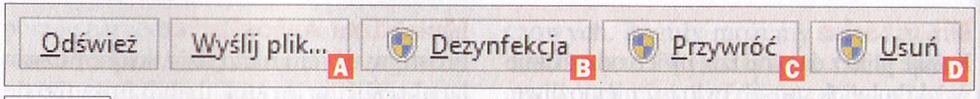


2 Wyświetlone zostanie okno dialogowe, w którym, klikając na , potwierdzamy chęć wyleczenia pliku.

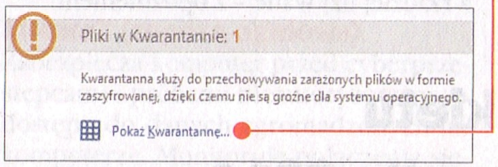


3 Jeśli leczenie się nie powiedzie, plik zostanie umieszczony w Kwarantannie. Dostęp do listy zapisanych w niej plików uzyskamy w głównym oknie

Więcej na: www.ebook4all.pl



aplikacji, klikając na zakładkę ●, a potem na ●. Otworzy się wówczas okno, w którym



zobaczymy listę zarażonych plików. Do dyspozycji mamy także szereg opcji:

A Wysłanie pliku do laboratorium G Daty w celu zbadania.

B Ponowną próbę dezynfekcji (może się to udać na przykład po kilku dniach, gdy twórcy programu zaktualizują bazy o odpowiednie procedury naprawcze).

C Kliknięcie na ten przycisk spowoduje przywrócenie pliku do jego oryginalnej lokalizacji.

D Ta opcja całkowicie usuwa z dysku zarażony plik.

Ręczne skanowanie

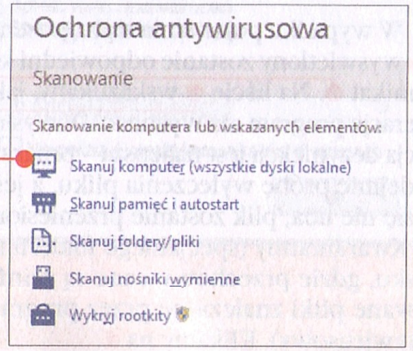
Mimo pracy Strażnika warto od czasu do czasu ręcznie przeskanować wszystkie dyski lub aktywować funkcję wykrywania rootkitów (czyli szkodników, które celowo ukrywają się przed antywirusem). Potrzebne opcje znajdziemy po kliknięciu na ●.

1 Klikając na ●, włączymy pełny skan całego systemu. Warto go wykonać na przykład bezpośrednio po zainstalowaniu programu antywirusowego. Za pomocą kolejnych opcji możemy zbadać stan pamięci operacyjnej i autostartu, wybranych folderów, nośników wymiennych. Wykrywanie rootkitów umożliwia ostatnia opcja – aby z niej skorzystać, musimy być zalogowani do Windows jako użytkownik z uprawnieniami administratora, w przeciwnym razie moduł antywirusa nie uzyska dostępu do chronionych obszarów systemu.

2 Skanowanie wybranych elementów możemy także wykonać, klikając na dysk, folder lub plik prawym przyciskiem myszy i z dostępnego menu kontekstowego wybierając opcję ●.

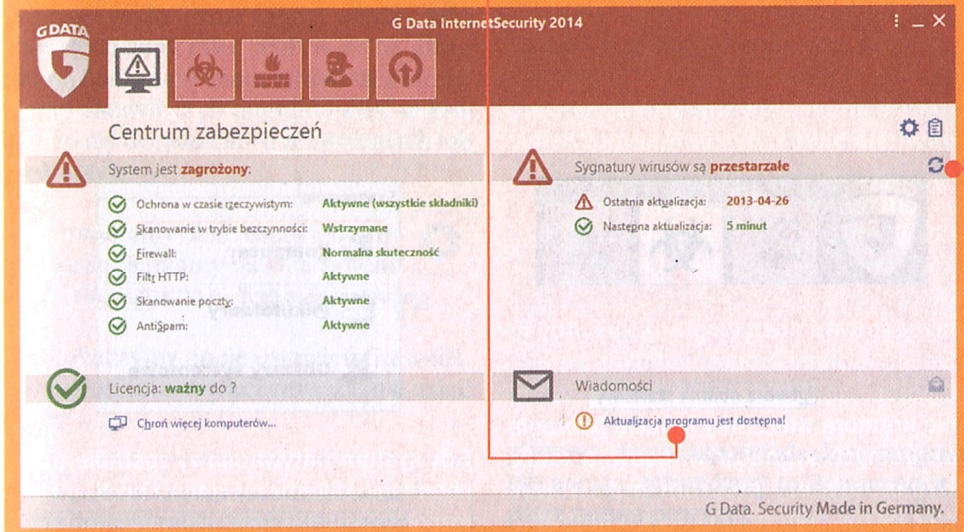
Optymalizacja pracy skanera

Ochroną w czasie rzeczywistym zarządza Strażnik G Data. Większość współczesnych komputerów poradzi sobie z maksymalnym poziomem ochrony. Gdy nasz komputer jest jednak bardzo wolny, należy tak skonfigurować funkcję skanowania, by zminimalizować obciążenie systemu, ale bez wyłączania skanowania w tle. Skuteczność antywirusa dobierzemy, wykonując następujące kroki.



DBAJ O AKTUALIZACJE

Co nam po programie do zabezpieczeń, jeśli jest nieaktualny? Nie chroni nas wówczas przed najnowszymi – a więc najbardziej niebezpiecznymi – zagrożeniami. W wypadku programu G Data InternetSecurity 2014 aktualizacje odbywają się automatycznie w tle, a więc bez naszego udziału. Jeśli jednak zauważymy, że dostępne są nowe aktualizacje programu lub sygnatur wirusów, kliknijmy na lub ●, by jak najszybciej przeprowadzić proces uaktualnienia. Podniesiemy w ten sposób poziom ochrony naszego peceta.

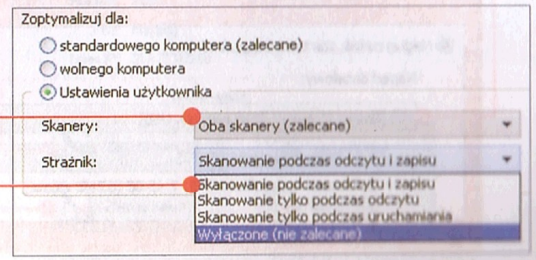


1 W oknie programu klikamy na ●, a potem na liście ▸ Ogólne wybieramy ●. Zaznaczamy opcję ◉ Ustawienia użytkownika.

▸ Skuteczność / Szybkość

2 Wybieramy liczbę aktywnych skanerów ●.

3 Następnie wskazujemy najwyższy poziom aktywności Strażnika – w tym celu zaznaczamy opcję ●. Kolejne ustawienia to coraz mniejszy poziom zabezpieczeń, ale i mniejsze obciążenie systemu. Wyłączenie Strażnika oznacza, że program antywirusowy będzie skanował pliki tylko na nasze żądanie, co nie jest zalecane. Zmiany zatwierdzamy, klikając na Zastosuj.

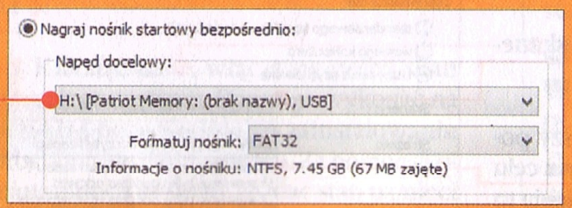


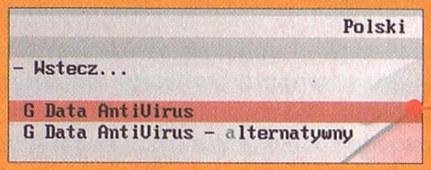
Więcej na: www.ebook4all.pl

RATUNKOWY NOŚNIK STARTOWY

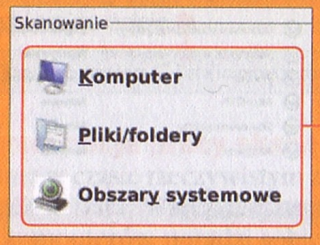
Może się zdarzyć, że w wyniku działania szczególnie groźnych szkodników system Windows nie będzie w stanie się uruchomić. W takim wypadku warto mieć w pogotowiu płytę startową lub rozruchowy pendrive z systemem antywirusowym. Za pomocą takiego nośnika uruchomimy specjalne środowisko, w którym będziemy mogli przeskanować system i wykasować znalezione szkodniki. Jeśli mamy zainstalowany pakiet G Data InternetSecurity, możemy samodzielnie

przygotować nośnik ratunkowy. Aby to zrobić, w oknie programu klikamy na ●, a potem na Utwórz nośnik startowy. W oknie kreatora włączamy funkcję pobrania aktualnych sygnatur wirusów, a także wybieramy, czy program ma tworzyć plik ISO w celu późniejszego nagrania go na płytę CD, czy też wolimy od razu stworzyć nośnik CD lub pendrive – w tym wypadku z listy wybieramy literę przypisaną do nagrywarki lub podłączonego do portu USB pendrive'a ● (wszystkie dane zapisane na nośniku wymiennym zostaną wykasowane).





Za pomocą gotowego nośnika, zgodnie z instrukcją obsługi płyty głównej naszego komputera, wykonujemy rozruch peceta. W menu startowym wybieramy język polski, a potem opcję ● i zatwierdzamy ją, wciskając enter.



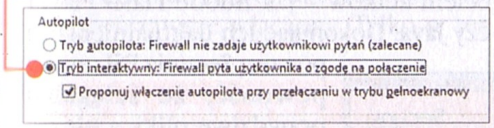
Gdy system antywirusowy zostanie uruchomiony, klikamy na jedną z opcji ●, aby rozpocząć skanowanie i usuwanie wirusów z dysku. Proces wyszukiwania szkodników może potrwać od kilku do nawet kilkudziesięciu minut. Warto pamiętać, że w wypadku, gdy nośnik utworzyliśmy jakiś czas temu, należy przeprowadzić jego aktualizację – zrobimy to na zakładce Aktualizacja. W wyświetlonym oknie musimy jednak podać numer licencji otrzymany e-mailem podczas rejestracji pakietu (patrz strony 100–101), a także dane logowania do serwerów aktualizacji (otrzymaliśmy je w oddzielnej wiadomości e-mail od firmy G Data).

Korzystanie z firewalla

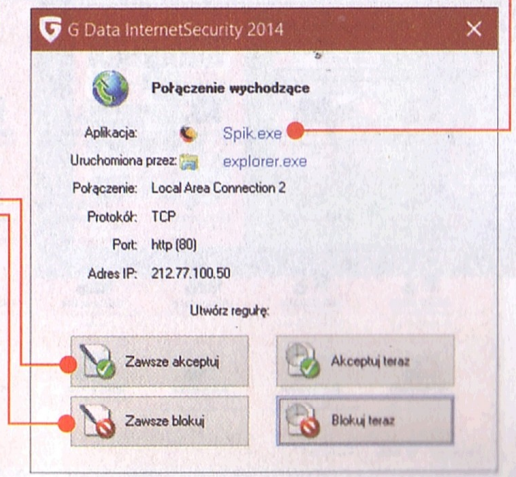
Zapora ogniowa wbudowana w pakiet G Data InternetSecurity 2014 domyślnie działa w trybie autopilota. Oznacza to, że program samodzielnie podejmuje decyzje dotyczące zezwalania lub blokowania połączeń przychodzących i wychodzących. W wypadku mniej doświadczonych użytkowników ta opcja jest zalecana – nie wymaga praktycznie żadnej wiedzy. Jeśli jednak chcemy mieć wpływ na to, które usługi i programy mogą łączyć się z siecią, warto ustawić tryb interaktywny, w którym to my decydujemy o zezwoleniach lub blokadach.

1 Otwieramy okno ustawień firewalla. Klikamy na ●, a potem na ▸ Firewall i na ▸ Tryb automatyczny.

2 Zobaczymy opcje ustawień firewalla. Autopilota wyłączymy, zaznaczając opcję ●.



3 Od teraz dla każdego programu lub procesu, który będzie usiłował nawiązać połączenie sieciowe, będzie wyświetlane okno kreatora reguł firewalla. Możemy w nim utworzyć zasadę stałej akceptacji połączeń ● lub stałej blokady ●. Pozostałe dwa przyciski umożliwiają tymczasowe zezwolenie na realizowanie połączeń lub ich zablokowanie. Oczywiście na samym początku po wyłączeniu autopilota takich powiadomień otrzymamy bardzo dużo – pamiętajmy, by zezwoleń udzielać tylko programom i usługom, które znamy i wiemy, że są bezpieczne. Jeśli mamy wątpliwości, za co odpowiada dany program lub usługa, sprawdźmy to w internecie – patrz ramka powyżej.



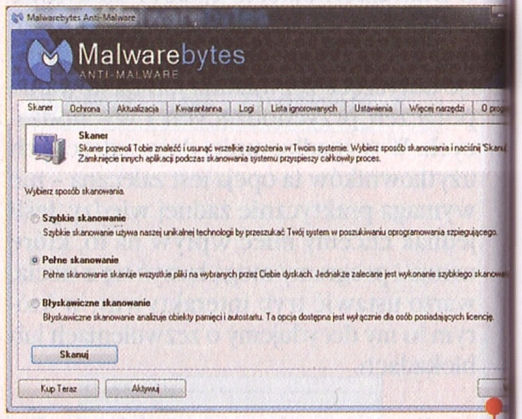
SPRAWDZANIE PROCESÓW

Jeśli w oknie kreatora reguł firewalla zobaczymy nazwę programu lub usługi, która nie jest nam znana, sprawdźmy, czy nie jest dziełem wirusa. Możemy w tym celu skorzystać z internetowych baz procesów – na przykład **pl.systemexplorer.net**, **www.process-information.net** lub **www.whatsrunning.net**. Na podanych stronach wyszukajmy nazwę podejrzanej aplikacji widoczną w polu ● – znajdziemy informacje o procesie lub aplikacji. Na podstawie opisów i oznaczeń nawet bez znajomości języka angielskiego można domyślić się, czy mamy do czynienia z zaufanym i bezpiecznym programem lub usługą, czy też lepiej będzie w tym wypadku zablokować możliwość nawiązywania połączeń sieciowych.

Więcej na: www.ebook4all.pl

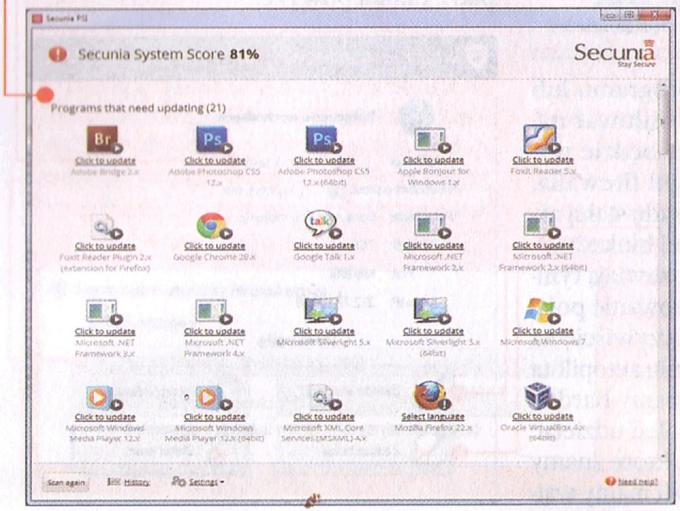
Dodatkowe zabezpieczenia

Instalacja i odpowiednie skonfigurowanie dobrego pakietu bezpieczeństwa to podstawa, ale by podnieść poziom bezpieczeństwa naszego komputera, powinniśmy wyposażyć go jeszcze w inne przydatne programy. Poznajmy najważniejsze z nich.



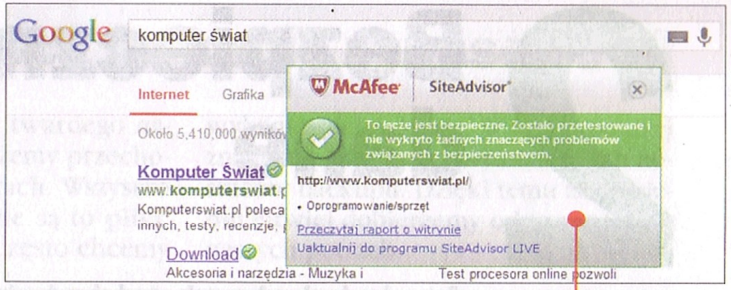
Secunia PSI

Niedbałość programistów lub zwykłe, przypadkowe błędy w aplikacjach powodują, że narzędzia, z których korzystamy na co dzień, często pełne są luk w zabezpieczeniach, przez które szkodliwy kod może wniknąć do naszego peceta. Jak sobie z tym poradzić? To proste – wystarczy zawsze korzystać z najnowszych dostępnych wersji programów. Tylko kto ma czas i chęć, żeby nieustannie śledzić aktualizacje? Na szczęście w tym nudnym i nieprzyjemnym zadaniu wyręczy nas program Secunia PSI (TYLKO W KŚ+). Aplikacja zbiera informacje o tym, z których programów korzystamy, i sama wyszukuje w internecie nowe wersje, które możemy ściągnąć za pomocą jednego kliknięcia. Szczególnie przydatne jest to w wypadku aktualizacji programów, które często są celem ataków – jak Adobe Flash Player czy Java. Dokonując ich uaktualnienia za pomocą Secunia PSI, mamy pewność, że ściągamy prawdziwe pliki, a nie zakamuflowane szkodniki.



Malwarebytes Anti-Malware

Bardzo prosty w obsłudze program, który spełnia podobne funkcje jak antywirus, ale swym działaniem obejmujące nieco inne spektrum zagrożeń. W darmowej wersji niedostępna jest **ochrona rezydentna***, działa jedynie skaner na żądanie. To jednak wystarczy, by choć raz w tygodniu wykonać dogłębne wyszukiwanie szkodników, które mogły umknąć używanemu przez nas antywirusowi. Program instalujemy z KŚ+ lub płyty dołączonej do książki (w menu krążka podajmy CD-KOD: 016).



SiteAdvisor

Dodatek do przeglądarek stron WWW, który informuje nas, czy witryna, którą odwiedzamy, jest bezpieczna i zaufana. Aplikacja dodaje także swoje oznaczenia do wyników wyszukiwania w Google – od razu więc widzimy, na które strony lepiej nie wchodzić, by nie narażać komputera na niebezpieczeństwo. Program możemy zainstalować za pomocą aplikacji KŚ+.

Aktualizacje Windows

Wbudowany w system Windows mechanizm Automatycznych aktualizacji powinien być zawsze włączony. Tylko w ten sposób bowiem zapewnimy pobieranie i instalację wszystkich ważnych poprawek do systemu – większość z nich to poprawki bezpieczeństwa, które łatają wykryte luki, przez które na dysk mogą przenikać szkodliwe programy.

APLIKACJA KŚ+

Na płycie dołączonej do książki lub na stronie **ksplus.komputerswiat.pl** znajdziemy program KŚ+. Ta aplikacja zawiera Wirtualną Płytę – kopię krążka dołączonego do książki, wzbogaconą o dodatkowe aplikacje. Aby z niej skorzystać, zakładamy konto i w oknie aplikacji klikamy na Zarejestruj nowy kod i wpisujemy kod nadrukowany na etykiecie płyty dołączonej do książki. Aplikacja KŚ+ to także doskonałe źródło sprawdzonych aplikacji, bezpiecznych do zainstalowania, i wirtualny kiosk, w którym można kupować różne tytuły czasopism z rodziny Komputer Świata i specjalne wydania premium. Poradnik do aplikacji KŚ+ znajdziemy w każdym numerze magazynu Komputer Świat.

* Wyjaśnienie pojęcia w leksykonie na stronach 102–103

Więcej na: www.ebook4all.pl

2 Bezpieczne dane

Awaria dysku twardego lub utrata komputera może się przydarzyć w każdej chwili. Dlatego konieczne jest skuteczne zabezpieczenie najważniejszych danych

Ważne dane możemy zabezpieczać na kilka sposobów, zależnych od stopnia ważności plików, ich liczby, rozmiarów oraz środków technicznych i finansowych, którymi dysponujemy. Kopie plików zajmujących dużo miejsca, czyli kolekcje zdjęć, filmów, duże pliki projektów, powinniśmy wykonywać na dysku zewnętrznym. Dysk o pojemności 2 TB (2000 GB) w obudowie podłączanej do komputera przez USB 3.0 można kupić już za mniej więcej 300 złotych.

Najbezpieczniejszym sposobem wykonywania kopii zapasowych jest **backup online***, czyli na wydzielonym dla nas fragmencie dysku usługodawcy w internecie. Profesjonalne usługi tego typu są płatne, ale warto zapłacić kilkadziesiąt złotych rocznie za bezpieczne przechowywanie bardzo ważnych dokumentów, które w każdej chwili możemy odzyskać.

Nie mniej ważna od bezpieczeństwa plików jest sprawność systemu Windows. Kopię systemu możemy w łatwy sposób regularnie wykonywać i w razie awarii przywracać system do pełnej sprawności o wiele szybciej niż trwa reinstalacja i ponowne instalowanie wszystkich potrzebnych programów. **pg**

DROGOWSKAZ

- Wybór miejsca na kopie zapasowe s. 21
- Kopia dużych zbiorów plików s. 22
- Backup w chmurze s. 24
- Kopia zapasowa systemu Windows s. 27
- Odświeżanie Windows 8 s. 29

PRZYDATNE PROGRAMY

- Cobian Backup — CD-KOD: 004
- Easeus Todo Backup — TYLKO W KS+

* Wyjaśnienie pojęcia w leksykonie na stronach 102–103

Wybór miejsca na kopie zapasowe

Kopie plików z dysku twardego naszego komputera możemy przechowywać w różnych miejscach. Wszystko zależy od tego, jak ważne są to pliki, ile miejsca zajmują i jak często chcemy wykonywać ich kopie. W tabeli poniżej znajdziemy wady i zalety możliwych nośników backupu. Dzięki temu zestawieniu łatwiej dobierzemy odpowiedni do naszych potrzeb.

ZALETY I WADY RÓŻNYCH LOKALIZACJI BACKUPU

	ZALETY	WADY
Partycja inna niż systemowa	■ brak dodatkowych kosztów ■ duża wygoda	■ niski poziom bezpieczeństwa kopiowanych danych
Inny dysk twardy w komputerze	■ duże bezpieczeństwo danych ■ duża szybkość zapisu	■ konieczność zakupu dysku ■ brak możliwości zamontowania drugiego dysku w notebooku
Zewnętrzny dysk twardy	■ łatwe podłączanie i odłączanie ■ mniejsze ryzyko utraty dysku w razie kradzieży komputera	■ konieczność zakupu dysku ■ konieczność podłączania dysku w czasie wykonywania kopii
Płyta CD lub DVD	■ duża dostępność nośników ■ niski koszt płyt ■ łatwe nagrywanie	■ mała pojemność płyt ■ żywotność nośników na poziomie kilku do kilkunastu lat ■ konieczność opisywania i katalogowania płyt
Pendrive	■ niski koszt zakupu ■ mobilność i poręczność nośników	■ stosunkowo mała pojemność ■ duże ryzyko zgubienia
Dysk sieciowy	■ kopia nie zabiera miejsca na dyskach lokalnych	■ skomplikowana konfiguracja ■ dysk sieciowy musi być cały czas dostępny
Serwer FTP	■ dostęp do danych przez internet	■ skomplikowana konfiguracja serwera ■ skomplikowany dostęp do danych ■ konieczność zakupu hostingu
Dysk internetowy	■ wygoda wykonywania kopii ■ łatwość instalacji	■ duże ryzyko przypadkowego skasowania lub nadpisania plików
Backup online	■ duże bezpieczeństwo danych ■ łatwe przywracanie ■ dostęp do danych przez internet	■ opłata abonamentowa za korzystanie z usługi

G DATA
Eksperci G Data radzą
Twórz kopie zapasowe. Backup pozwala zapisać ważne dane na wypadek awarii systemu.
G DATA

Więcej na: www.ebook4all.pl

Kopia dużych zbiorów plików

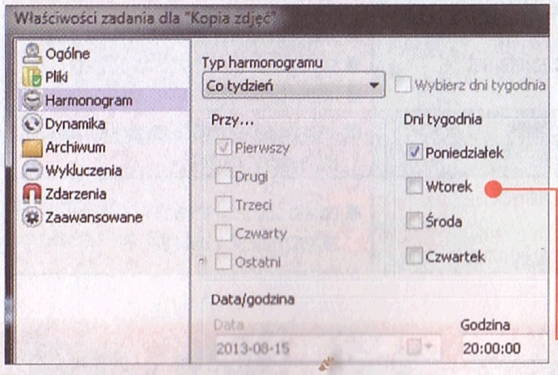
Na dyskach naszych komputerów gromadzimy coraz więcej ważnych plików. Przechowujemy na nich dokumenty formalne, ale również mające dużą wartość sentymentalną kolekcje zdjęć z aparatów cyfrowych i plików z prywatnymi filmami. Niestety, rzadko kto zastanawia się, co się stanie z jego ważnymi plikami w razie awarii dysku bądź zniszczenia lub utraty komputera. Jedyne kopie plików po prostu przepadną, a wraz z nimi wspomnienia z wielu lat i ważne informacje. Dlatego też należy regularnie wykonywać kopie zapasowe danych.
Zobaczmy, jak zadbać o bezpieczeństwo plików o dużych rozmiarach lub dużych zbiorów plików.

Jaki program do backupu

Jest wiele programów, które służą do automatycznego wykonywania kopii zapasowych wybranych przez użytkownika plików. Na płycie dołączonej do książki (lub na Wirtualnej Płycie w aplikacji KŚ+) znajdziemy kilka takich pozycji, na przykład Cobian Backup (CD-KOD: 004), który umożliwia tworzenie wielu zadań kopii oraz ma funkcję **kompresji*** oraz szyfrowania kopii. Wszystkie te aplikacje działają podobnie. Tworzymy w nich zadania, w ramach których wskazujemy pliki przeznaczone do kopiowania, wybieramy lokalizację docelową oraz ustalamy harmonogram, według którego kopia będzie automatycznie wykonywana. Jeśli nie chcemy instalować dodatkowych programów do backupu, możemy skorzystać z wbudowanego w Windows narzędzia Kopia zapasowa.

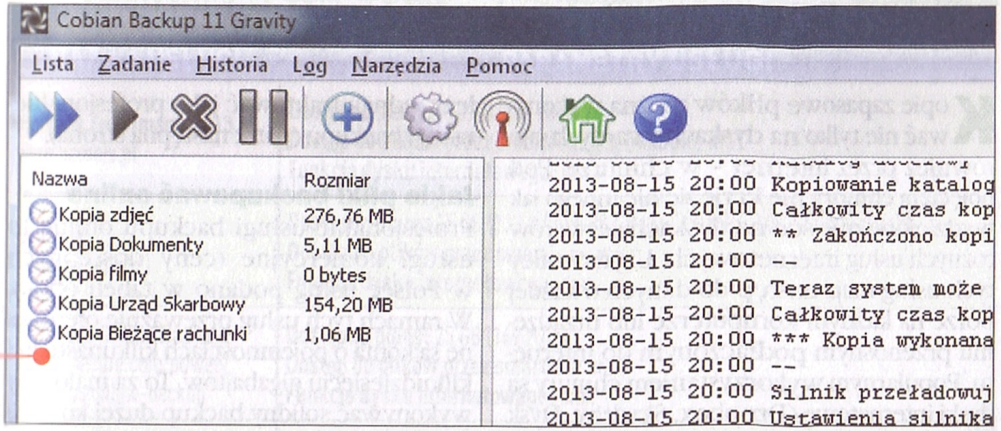
Gdzie przechowywać kopie

Kopię zapasową zbiorów plików zajmujących dużo miejsca (na przykład kolekcji zdjęć czy filmów) powinniśmy wykonywać na dysku zewnętrznym. Nie wystarczy kopiować danych na inną partycję dysku systemowego, ponieważ w razie awarii dysku, co może zdarzyć się w każdej chwili, stracimy nasze pliki.
Jeśli backup wykonujemy na komputerze stacjonarnym, w którym mamy zamontowany dodatkowy dysk twardy, kopie plików możemy zapisywać na tym dysku zamiast na dysku zewnętrznym.



Jak często wykonywać kopię

Częstotliwość wykonywania kopii powinna zależeć od tego, jak często i jak bardzo powiększa się zbiór plików przeznaczonych do backupu oraz jak ważne są to pliki. Jeżeli codziennie przybywa nam w kolekcji wiele ważnych plików, wtedy w harmonogramie kopii ustawiamy codzienne wykonywanie kopii o określonej godzinie. Oczywiście komputer musi być w tym czasie włączony. Jeśli komputer jest wyłączony o godzinie, którą wyznaczyliśmy jako godzinę kopiowania, kopia zostanie wykonana po włączeniu komputera. Jeżeli ważnych plików przybywa na dysku rzadko, w harmonogramie kopii ustawiamy częstotliwość tygodniową lub miesięczną.
Programy do backupu umożliwiają również uruchomienie zadania kopii zapasowej na żądanie. Jednak tę możliwość pozostawmy na wyjątkowe wypadki, a polegajmy raczej na automatycznym, regularnym wykonywaniu kopii przez program.



Oddzielne zadania dla różnych plików

Większość programów do backupu, na przykład Cobian Backup, który znajdziemy na płycie oraz w aplikacji KŚ+, umożliwia stworzenie wielu niezależnych zadań kopii. Każde zadanie może dotyczyć różnych folderów i różnych rodzajów plików. Tak więc można na przykład stworzyć zadanie dla folderu ze zdjęciami, który będzie kopiowany raz w tygodniu, a oddzielne zadanie będzie realizowało codzienny backup folderu Dokumenty, w którym znajdują się pliki edytowane na co dzień.

Różne rodzaje kopii

Programy do backupu umożliwiają wykonywanie różnego rodzaju kopii. Jeżeli wybierzemy kopię pełną, wtedy za każdym razem, kiedy według harmonogramu będzie wykonywany backup, będą kopiowane wszystkie pliki ze wskazanych folderów, a pliki zapisane na dysku docelowym będą nadpisywane.
Zadaniem kopii przyrostowej będzie kopiowanie tylko nowych plików oraz plików, które zostały zmodyfikowane od czasu wykonania ostatniej kopii.
Zasada działania kopii różnicowej jest podobna do kopii przyrostowej, ale wykonywana jest kopia plików nowych i zmodyfikowanych od czasu wykonania ostatniej pełnej kopii.
Najlepszym wyborem w większości wypadków jest wykonywanie kopii przyrostowej.

* Wyjaśnienie pojęcia w leksykonie na stronach 102-103

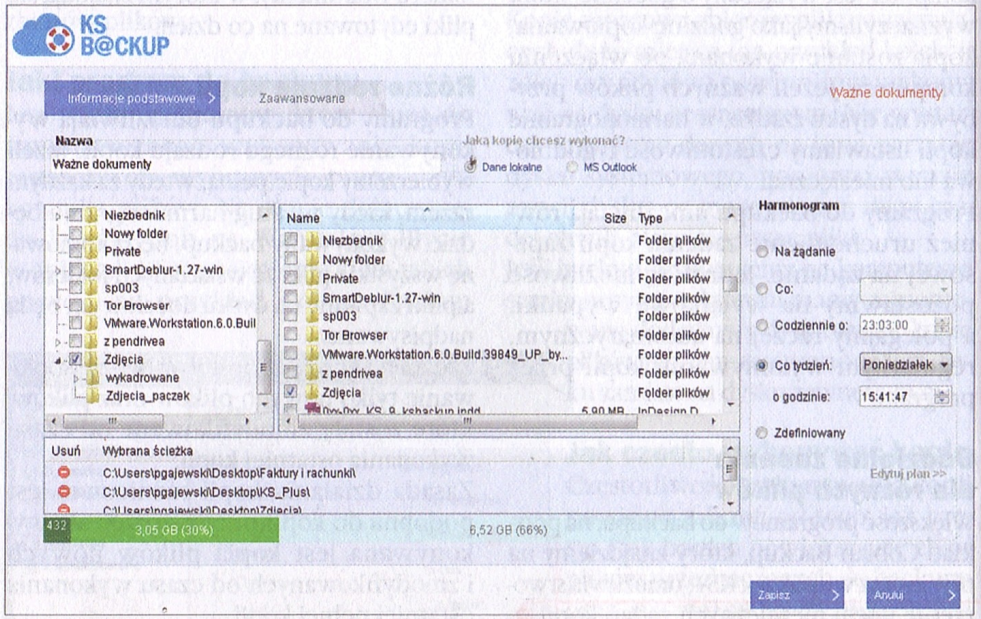
Więcej na: www.ebook4all.pl

Backup w chmurze

Kopie zapasowe plików można wykonywać nie tylko na dyskach twardych, ale również przez internet – w chmurze. Pod pojęciem chmury nie kryje się nic innego jak wydzielone miejsce na dyskach serwerów różnych usług internetowych. Użytkownicy tych usług mają dostęp do danych o każdej porze na każdym komputerze lub urządzeniu przenośnym podłączonym do internetu. Popularnym wykorzystaniem chmury są dyski internetowe (Dropbox, Skydrive, Dysk Google czy 4sync), gdzie wszystkie zmiany w zawartości folderu na dysku twardym są odzwierciedlane na dysku internetowym, i odwrotnie. Dysku internetowego nie należy jednak traktować jako profesjonalnej usługi backupu (patrz następna strona).

Jakie pliki backupować online

Profesjonalne usługi backupu online to usługi komercyjne (ceny dostępnych w Polsce usług podano w tabeli obok). W ramach tych usług przeważnie oferowane są konta o pojemnościach kilkunastu lub kilkudziesięciu gigabajtów. To za mało, aby wykonywać solidny backup dużej kolekcji zdjęć czy innych dużych plików. Jednak na ważne dokumenty tekstowe, skany faktur czy małe pliki projektów kilkanaście gigabajtów w zupełności wystarczy.



W profesjonalnych usługach backupu online, na przykład w KS Backup, do dyspozycji mamy program, w którym możemy ustawić wiele niezależnych zadań backupu, wykonujących kopie różnych grup plików z zadaną przez nas częstotliwością

PORÓWNANIE PARAMETRÓW USŁUG BACKUPU ONLINE

NAZWA USŁUGI	PARAMETRY USŁUGI
Acronis True Image 2013 www.acronis.pl	**Dostępne plany:** 250 GB (210 zł/rok) **Dostęp do plików przez smartfon:** jest (Android, iOS) **Funkcja dysku internetowego:** jest
BitBank (www.bitbank.pl)	**Dostępne plany:** 15 GB (130 zł/rok), 30 GB (250 zł/rok), 100 GB (500 zł/rok) **Dostęp do plików przez smartfon:** brak **Funkcja dysku internetowego:** brak
F-Secure Online Backup www.f-secure.com/pl/web/home_pl/online-backup	**Dostępne plany:** 25 GB (169 zł/rok) **Dostęp do plików przez smartfon:** brak **Funkcja dysku internetowego:** brak
iBARD24 www.ibard24.pl	**Dostępne plany:** 10 GB (199 zł/rok) **Dostęp do plików przez smartfon:** jest (Android, iOS) **Funkcja dysku internetowego:** jest
KS Backup www.ksbackup.komputerswiat.pl	**Dostępne plany:** 5 GB (30 zł/rok), 10 GB (52 złote/rok) **Dostęp do plików przez smartfon:** jest (Android, iOS) **Funkcja dysku internetowego:** jest

Dlaczego nie używać dysku internetowego do backupu

Usługa backupu w chmurze powinna być odpowiednikiem programu do wykonywania kopii zapasowej na dysku twardym. Powinniśmy więc mieć możliwość wyboru danych, które mają być kopiowane, tworzenia oddzielnych zadań backupu dla różnego rodzaju plików oraz ustalania harmonogramu kopii. Dyski internetowe działają natomiast na zasadzie synchronizacji folderów – jeden z nich jest na dysku twardym, natomiast drugi na dysku serwera. Jeżeli więc ważny plik skasujemy z jednego z tych katalogów, natychmiast zostanie również usunięty z drugiego. Na większości dysków internetowych możliwe jest przywrócenie skasowanych plików bądź odzyskanie nadpisanej wersji dokumentu, ale przecież nie o to chodzi w backupie.

Jakie funkcje ma dobry backup online

Profesjonalnych usług backupu online jest niewiele i różnią się od siebie parametrami i ceną. Aby wybrać dobre rozwiązanie, oprócz ceny abonamentu należy kierować się kilkoma ważnymi czynnikami:

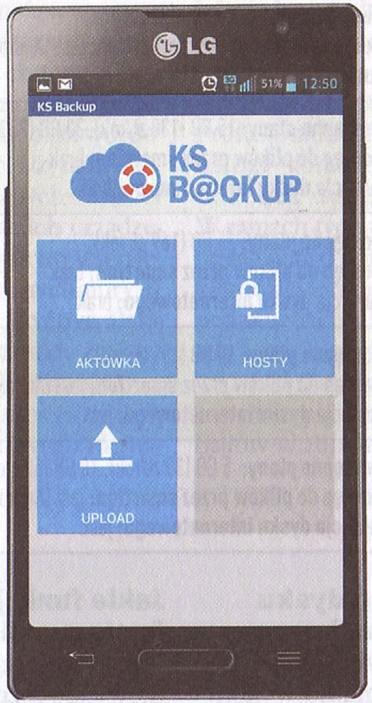
- **Bezpieczeństwo** – serwery usług backupu online, jak wszystkie inne komputery, nie są niezawodne. Dlatego najlepszym zabezpieczeniem przed utratą plików jest wykonywanie na bieżąco kopii na innym serwerze. Technikę taką nazywamy **redundancją*** i jest ona stosowana w wielu usługach internetowych, na przykład w KS Backup. Dzięki temu w razie awarii jednego z serwerów usługodawcy mamy natychmiastowy dostęp do danych na drugim serwerze.

* Wyjaśnienie pojęcia w leksykonie na stronach 102–103

Więcej na: www.ebook4all.pl

- **Rozmiar konta** – miejsce na kopie zapasowe na serwerach usługodawców jest dość drogie (patrz tabela na poprzedniej stronie). Dlatego wybierając usługę backupu, zastanówmy się wcześniej, jakie dane będziemy backupować. Na ważne dokumenty, na przykład pliki związane z pracą, faktury, rachunki czy dokumenty urzędowe, wystarczy w zupełności kilkanaście gigabajtów. Do porządnego backupu kolekcji zdjęć i filmów potrzeba kilkuset gigabajtów, więc albo będziemy słono płacić za miejsce na serwerach, albo wybierzmy inną metodę, na przykład kopiowanie plików na dysk zewnętrzny (patrz strony 22–23).

- **Dostęp do plików online** – dostęp do skopiowanych plików powinniśmy mieć zawsze i wszędzie. Wszystkie usługi backupu online pozwalają ściągać pliki po zalogowaniu się na swoje konto w usłudze w przeglądarce internetowej. Dobrze również, jeśli do dyspozycji mamy dedykowaną aplikację na smartfon, która ułatwia zarządzanie plikami.



Niektóre usługi backupu online oferują dodatkowo funkcję dysku internetowego. Podobnie jak w innych usługach tego typu zawartość wskazanego na dysku folderu jest synchronizowana z folderem przechowywanym na serwerze. Na ilustracji obok aplikacja mobilna KS Backup z funkcją Aktówka

10 GB ZA DARMO NA ROK W USŁUDZE KS BACKUP

Komputer Świat we współpracy z Opero – profesjonalną firmą oferującą rozwiązania backupu online – przygotował dla Czytelników specjalną ofertę, w ramach której można otrzymać za darmo na rok 10 GB miejsca na backup w serwisie KS Backup pod adresem **ksbackup.komputerswiat.pl**. Po upływie roku Czytelnicy będą mogli przedłużyć ważność konta o kolejny rok za gwarantowaną kwotę 30 złotych.

Kod na darmowe 10 GB na rok w KS Backup znajdziemy w Strefie Bonus Komputer Świata 9/2013 (e-wydanie czasopisma możemy kupić w aplikacji KŚ+ pod adresem **ksplus.komputerswiat.pl**). Kod można zarejestrować do końca 2013 roku.

Kopia zapasowa systemu Windows

Niestety, prawdą jest, że Windows może zacząć działać niestabilnie w każdej chwili, a odnalezienie przyczyny problemów jest czasem niezwykle trudne i czasochłonne. Dlatego wielu użytkowników w takich wypadkach decyduje się na reinstalację systemu. Chociaż samo ponowne zainstalowanie Windows nie zajmuje wiele czasu, to skonfigurowanie systemu i instalowanie wszystkich używanych wcześniej programów pochłania bardzo dużo czasu i energii. Lepszym rozwiązaniem jest wykonanie kopii całej partycji systemowej wraz z programami na zewnętrznym dysku. W razie problemów z systemem przywrócimy jego stan z dnia wykonania kopii wraz z wszystkimi plikami znajdującymi się w tym momencie na partycji systemowej.

Program do tworzenia kopii zapasowych został wbudowany w Windows. Niestety, narzędzie to często sprawia problemy. Dlatego Komputer Świat pokaże, jak wykonać i przywrócić kopię zapasową całej partycji systemowej za pomocą programu Easeus Todo Backup (TYLKO W KŚ+).

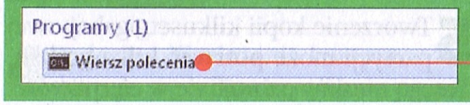
Tworzenie kopii zapasowej systemu

Kopię zapasową systemu najlepiej wykonywać na dysku zewnętrznym. Zanim rozpoczniemy tworzenie kopii na takim dysku, upewnijmy się, że jest na nim odpowiednio dużo wolnego miejsca. Na backup całego systemu operacyjnego potrzeba tyle miejsca, ile miejsca jest zajęte na partycji systemowej, czyli tej z zainstalowanym systemem. Dodatkowo musimy sprawdzić, czy dysk docelowy dla kopii jest sformatowany w systemie plików **NTFS***. Jeśli tak nie jest, zapoznajmy się z ramką u góry strony.

* Wyjaśnienie pojęcia w leksykonie na stronach 102–103

POTRZEBNY NTFS

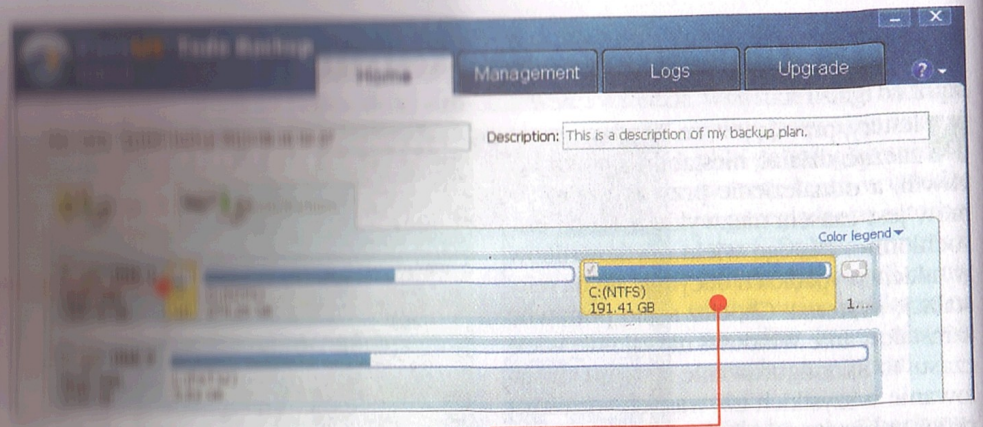
Dysk używany do przechowywania kopii zapasowej systemu musi być sformatowany w systemie plików NTFS. Wynika to z tego, że plik kopii jest bardzo duży, a na partycjach ze starszym systemem FAT32 można zapisywać pliki o maksymalnym rozmiarze 4 GB. Partycję dysku z systemem FAT32 łatwo możemy jednak konwertować na NTFS. Aby to zrobić, w pole wyszukiwania w menu Start wpisujemy **Wiersz polecenia***, klikamy prawym przyciskiem myszy na i wybieramy Uruchom jako administrator. W oknie Wiersza polecenia wpisujemy polecenie **convert [dysk]: /fs:ntfs** gdzie **[dysk]** oznacza literę partycji, którą konwertujemy, na przykład D. Konwersja rozpocznie się po naciśnięciu enter.



1 Podłączamy dysk, na którym zapiszemy kopię systemu, instalujemy za pomocą aplikacji KŚ+ (patrz strona 19) program Easeus Todo Backup i uruchamiamy go.

2 W głównym oknie programu klikamy na i następnie na System backup.

Więcej na: www.ebook4all.pl



3 Program wykryje partycję z zainstalowanym systemem Windows i oznaczy ją na żółto. W wypadku Windows 7 zostanie wykonany dodatkowo backup ukrytej 100-megabajtowej partycji.

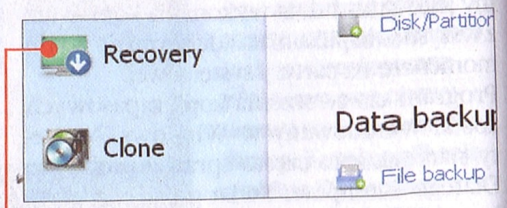
4 Aby rozpocząć wykonywanie kopii partycji systemowej, klikamy na przycisk Proceed.

5 Tworzenie kopii kilkusetgigabajtowej partycji może potrwać kilka godzin, dlatego musimy uzbroić się w cierpliwość. Kiedy proces dobiegnie końca, klikamy na przycisk Finish.

Przywracanie kopii systemu

Kiedy system zacznie sprawiać problemy i nie da się go naprawić w żaden znany nam sposób, przywracamy go z kopii, którą wykonaliśmy zgodnie z poprzednią wskazówką. **Uwaga!** Zostanie przywrócony obraz partycji systemowej, czyli wszystkie pliki znajdujące się na niej w momencie wykonania kopii. Jeśli chcemy zachować pliki, które zostały dodane po wykonaniu kopii systemu, musimy je przenieść na inny dysk, zanim rozpoczniemy przywracanie.

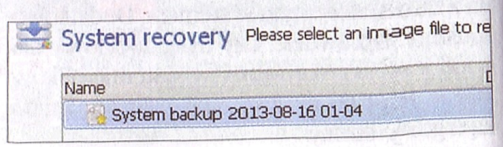
1 Podłączamy dysk, na którym znajduje się wykonana przez nas kopia systemu, i uruchamiamy program Easeus Todo Backup.



2 W głównym oknie programu klikamy na i następnie na System recovery.

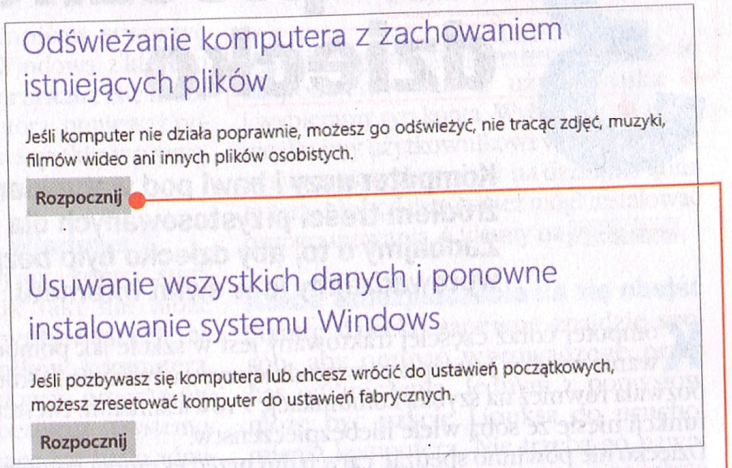
3 W kolejnym oknie kliknięciem wskazujemy kopię systemu, którą chcemy przywrócić, a w dwóch kolejnych oknach klikamy na Next.

4 Po kliknięciu na przycisk Proceed rozpocznie się przywracanie partycji systemowej z wykonanej przez nas kopii.

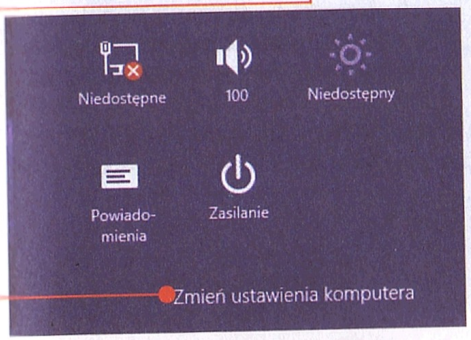


Odświeżanie Windows 8

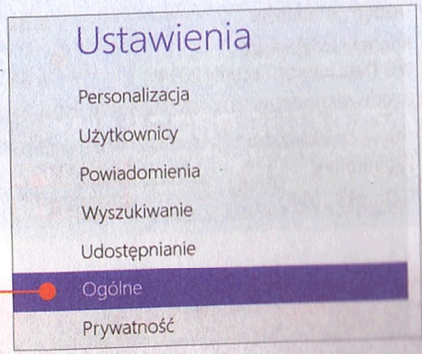
Kiedy Windows 8 zaczyna sprawiać problemy, nie musimy go ponownie instalować ani przywracać **obrazu partycji*** systemowej, jak ma to miejsce we wcześniejszych wersjach Windows. Ósemka jest pierwszym systemem Microsoftu, w którym zastosowano funkcję odświeżania systemu. Odświeżanie polega na ponownym zainstalowaniu systemu, ale z zachowaniem wszystkich plików, aplikacji zainstalowanych ze Sklepu Windows oraz wprowadzonych ustawień. Niestety, programy zainstalowane przez nas z innych źródeł niż Sklep zostaną usunięte. Zobaczmy, jak odświeżyć Windows 8.



1 Wciskamy jednocześnie klawisze i następnie klikamy na.



2 W lewej części okna ustawień systemu klikamy na.



3 Przewijamy zawartość wyświetlonego okna w dół i klikamy na przycisk. Następnie potwierdzamy rozpoczęcie procesu odświeżania systemu, klikając na przycisk Dalej, i w kolejnym oknie klikamy na Odśwież.

4 Podczas odświeżania komputer zrestartuje się kilka razy. Kiedy pojawi się okno logowania, odświeżony system jest gotowy do pracy. Cały proces nie powinien trwać dłużej niż kilkanaście minut.

* Wyjaśnienie pojęcia w leksykonie na stronach 102–103

Więcej na: www.ebook4all.pl

3 Bezpieczne dziecko

Komputer uczy i bawi pod warunkiem, że jest źródłem treści przystosowanych dla najmłodszych. Zadbajmy o to, aby dziecko było bezpieczne, i mądrze wprowadzajmy je w świat internetu

Komputer coraz częściej traktowany jest w szkole jak pomoc, narzędzie do zdobywania wiedzy. Jest lepszy i wygodniejszy w użyciu niż kilkutomowa encyklopedia, pozwala również na szybką komunikację z rówieśnikami. Niestety, obok pożytecznych funkcji niesie ze sobą wiele niebezpieczeństw.

Dziecko nie powinno spędzać całych dni przed ekranem komputera. Monitor nie wpływa korzystnie na wzrok, a siedząca pozycja przy biurku na kręgosłup. W słoneczne dni lepiej wysłać dziecko na boisko niż pozwolić grać mu w FIFĘ. Również same gry komputerowe nie wpływają dobrze na rozwój psychiczny dziecka. Jakże popularne krwawe tytuły FPP zacierają obraz rzeczywistości, przez co zdarzają się nawet tragiczne wypadki. Warto więc ograniczyć dostęp dziecka do komputera oraz nieodpowiednich gier i nie musimy tego robić poprzez zakazy lub przykre dyskusje. Używając odpowiednich narzędzi, stworzymy harmonogram dostępu dziecka do komputera i zablokujemy nieodpowiednie dla jego wieku gry. Warto zadbać również, aby dzieci nie miały dostępu do treści erotycznych, brutalnych, szerzących rasizm i ksenofobię, stron wykorzystujących różne formy psychomanipulacji. Są to pułapki dla osób dorosłych i na pewno przerastają zdolności adaptacyjne dziecka. Dlatego warto wiedzieć, jakie strony w internecie odwiedzają nasze pociechy, i w razie potrzeby potrafić je zablokować. **aś**

DROGOWSKAZ

- Zabezpiecz komputer s. 31
- Kontrola rodzicielska s. 32
- Dostęp do internetu s. 34
- Kontrola rodzicielska w G Data InternetSecurity 2014 s. 36

PRZYDATNE PROGRAMY

- Filtr rodzinny CD-KOD: 020
- G Data IS 2014 CD-KOD: 007

Eksperci G Data radzą

Ucz dzieci bezpiecznego korzystania z sieci i chr za pomocą funkcji kontroli rodzicielskiej.

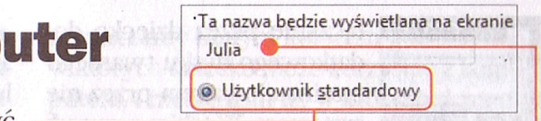
Zabezpiecz komputer

Na początek powinniśmy stworzyć konto w systemie Windows, z którego nasze dziecko będzie korzystało. Nie może to być konto administratora, ponieważ pozwalałoby obchodzić wszystkie wprowadzone przez nas zabezpieczenia.

Konto w systemie Windows 7

W Windows tworzymy konto standardowe. Użytkownik taki nie może wprowadzić zmian wpływających na wszystkich użytkowników komputera. Nie może także instalować programów i zmieniać ustawień zabezpieczeń systemowych. Do tego wymagane jest hasło administratora – musimy więc je stworzyć na koncie używanym przez siebie.

1 Klikamy na , a następnie na Panel sterowania, aby otworzyć okno z ustawieniami. W celu dodania nowego użytkownika klikamy na Dodaj lub usuń konta użytkowników.



2 Klikamy na Utwórz nowe konto, następnie podajemy nazwę użytkownika i wybieramy typ konta. Wybierając , uniemożliwimy użytkownikowi wprowadzanie zmian mających wpływ na działanie komputera, nie będzie również mógł instalować oprogramowania. Klikamy na Utwórz konto.

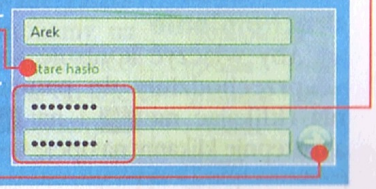
Każde zabezpieczenie da się obejść

Starsze dziecko zapewne znajdzie sposób, aby ominąć wprowadzone przez nas ograniczenia. Jednym z pomysłów może być użycie Linuksa do uruchomienia komputera. Nie trzeba go nawet instalować, wystarczy nagrać na płytę i uruchomić z niej pecet. Inny system użyty przez pociechę sprawi, że wszystkie wprowadzone przez nas ograniczenia nie będą miały zastosowania. Innym, jeszcze bardziej wyrafinowanym sposobem na ominięcie naszych zabezpieczeń jest pod-

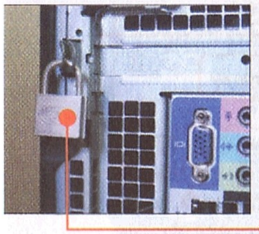
ZABEZPIECZAMY WŁASNE KONTO

Tworzenie konta dla dziecka nie będzie miało żadnego sensu, jeżeli nie zabezpieczymy swojego profilu z prawami administratora. Jeżeli będzie ono mogło zalogować się do naszego konta, bez problemu zainstaluje grę i będzie mogło do woli korzystać z zasobów internetu. Swoje konto najłatwiej zabezpieczyć hasłem. Aby to zrobić, w uruchomionym systemie Windows równocześnie wciskamy trzy klawisze – alt ctrl delete.

Następnie z wyświetlonego na ekranie menu wybieramy opcję Zmień hasło... Klikamy na ikonę swojego użytkownika i dwukrotnie podajemy hasło . Jeżeli dotąd konto nie było chronione hasłem, pole pozostawiamy puste. Klikamy na .



Więcej na: www.ebook4all.pl



łączanie przez dziecko dodatkowego dysku twardego z zainstalowanym przez nie systemem. W takim przypadku pozostaje nam zabezpieczyć obudowę komputera – na przykład małą kłódką.

Nie dla systemów LiveCD

Aby zabezpieczyć się przed uruchomieniem komputera za pomocą innego systemu operacyjnego, musimy zmienić ustawienia **BIOS-u***. W zależności od producenta płyty głównej nazwy ustawień i ich lokalizacje mogą się nieznacznie różnić.

1 Uruchamiamy ponownie komputer i zaraz po starcie wciskamy F10 lub F2, lub delete, aby przejść do ustawień BIOS-u.

2 Następnie przechodzimy do zakładki Configuration i do opcji ▸Boot Options. Następnie szukamy opcji CD-ROM Boot i zmieniamy ją na <Disabled>.

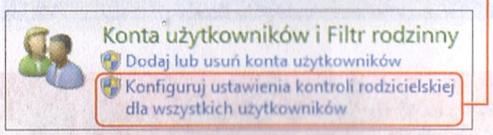
3 Żeby dziecko nie zmodyfikowało tych ustawień, zabezpieczymy BIOS hasłem. Przechodzimy do zakładki Security i za pomocą opcji Administrator Password ustawiamy hasło. Wciskamy F10, aby zapisać zmiany i wyjść z BIOS-u.

Kontrola rodzicielska

Mając odpowiednio zabezpieczony komputer, możemy przejść do ograniczeń, jakie nałożymy naszemu dziecku. Warto wcześniej zastanowić się nad nimi, dopasowując na przykład harmonogram dostępu do komputera do planu zajęć dziecka. Pamiętajmy, aby ograniczenia przedyskutować z dzieckiem. Zaleca się, aby dzieci poniżej 12 roku życia nie miały komputera w swoim pokoju, a dzieci w wieku poniżej 14 lat nie miały nieograniczonego dostępu do internetu.

Uruchomienie

1 Aby włączyć kontrolę rodzicielską, przechodzimy do panelu sterowania (klikając na i na Panel sterowania), a następnie klikamy na opcję.



2 Następnie wybieramy użytkownika, dla którego chcemy włączyć kontrolę rodzicielską, i w nowo otworzonym oknie klikamy na Włączona, egzekwuj bieżące ustawienia.

Limity czasu

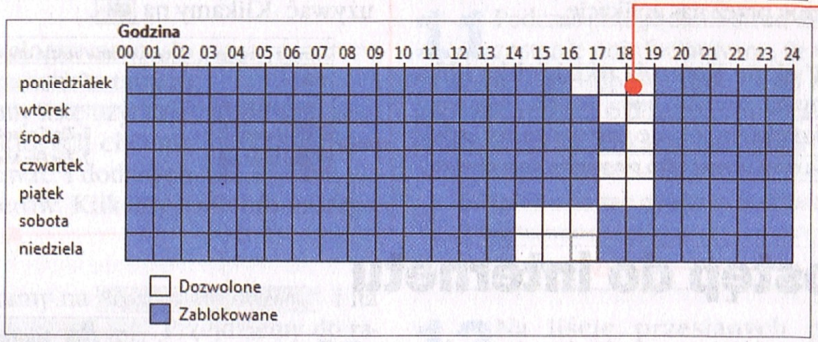
Kontrola rodzicielska w systemie Windows 7 ma trzy moduły: Limity czasu, Gry, Dozwalaj i blokuj określone programy. Zobaczmy, jak je skonfigurować.

1 Rozpoczniemy od ustalenia harmonogramu godzin, w których dziecko będzie mogło zalogować się do swojego konta i korzystać z komputera. Klikamy na Limity czasu.

2 Zaleca się, aby dzieci w wieku 3–5 lat przed komputerem spędzały nie więcej niż 20 minut dziennie, pół godziny dzieci chodzące do pierwszych klas szkoły podstawowej (6–10 lat), natomiast powyżej

* wyjaśnienie pojęcia w leksykonie na stronach 102-103

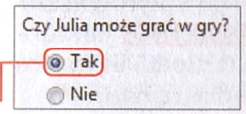
10 lat do godziny dziennie. Wszystkie te ustalenia powinny być jednak dostosowane do indywidualnych potrzeb i uwarunkowań. Na wyświetlonym planie tygodnia zaznaczamy białym kolorem godziny, w których dziecko może korzystać z komputera, i niebieskim te, w których dostęp będzie zabroniony. Klikamy na OK.



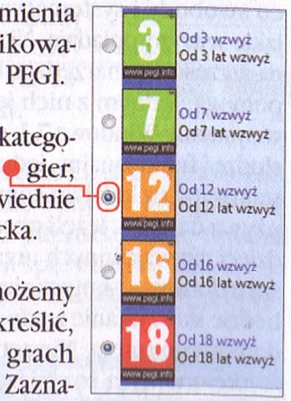
Kontrolujmy, w co dziecko gra

Sporym zagrożeniem są również gry. Wiele bardzo popularnych wśród dzieci tytułów przepełnionych jest brutalną, drastyczną i krwawą fikcją. Niestety, dzieci nie są w stanie skutecznie rozdzielić świata wirtualnego od rzeczywistego. Dlatego powinniśmy starannie dobierać gry, w które grają nasze pociechy. Z pomocą przychodzi nam europejski system klasyfikacji gier – w skrócie **PEGI**. Dzięki niemu gry dobieramy na podstawie kategorii wiekowej, możemy się również dowiedzieć, jakie potencjalnie niebezpieczne treści zawiera taka gra. Niestety, dzieci nie zawsze grają tylko w gry, które kupują im rodzice. Dużo częściej pożyczają je od znajomych, zdarza się, że w tajemnicy przed rodzicami. Aby mieć kontrolę nad uruchamianymi na domowym komputerze grami, skorzystamy z kolejnej funkcji kontroli rodzicielskiej.

1 W oknie konfiguracji kontroli rodzicielskiej klikamy na. Jeżeli chcemy zezwolić dziecku na uruchamianie gier, zaznaczamy opcję.

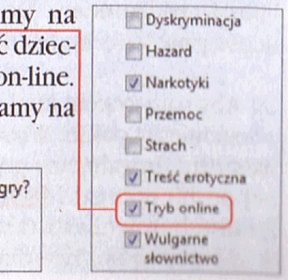


2 W kolejnym kroku konfigurujemy system klasyfikacji gier. Klikamy na Ustaw klasyfikacje gier i zaznaczamy Zablokuj gry niesklasyfikowane, aby nie dopuścić do uruchomienia gier niesklasyfikowanych w systemie PEGI.



3 Zaznaczamy kategorię wiekową gier, które będą odpowiednie dla naszego dziecka.

4 Poniżej zaś możemy dokładnie określić, jakie treści w grach będą blokowane. Zaznaczając, możemy na przykład zabronić dziecku gry w trybie on-line. Dwukrotnie klikamy na na OK.



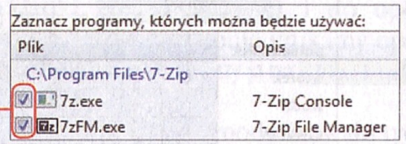
Więcej na: www.ebook4all.pl

Tylko dozwolone programy

Ostatnim elementem kontroli rodzicielskiej jest funkcja blokowania programów. Dzięki niej dziecko będzie mogło uruchamiać tylko wybrane przez nas aplikacje.

1 W oknie Kontrola rodzicielska klikamy na Dozwalaj i blokuj określone programy i w kolejnym oknie zaznaczamy opcję Julia może używać tylko programów dozwolonych.

2 Moduł kontroli rodzicielskiej przeskanuje system w poszukiwaniu programów. Z wyświetlonej listy zaznaczamy tylko te, których dziecko będzie mogło używać. Klikamy na OK.

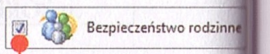


Dostęp do internetu

Najtrudniejszym zadaniem jest odpowiednie zabezpieczenie dostępu do internetu, tak żeby dziecko mogło odwiedzać tylko witryny adekwatne do jego wieku. Dobrze pozostawić naszym pociechom nieco swobody i systematycznie sprawdzać, jakie witryny oglądają. Nie jest to łatwe, ale na szczęście są narzędzia, które nam w tym pomogą. Jednym z nich jest Filtr rodzinny w systemie Windows 7. Jest wygodny w obsłudze i funkcjonalny, jednak musi być zainstalowany na każdym komputerze, którego używa dziecko. Jeżeli oprócz komputerów dzieci używają innych urządzeń – tabletów, smartfonów – skuteczniejszym sposobem będzie skorzystanie z odpowiedniej funkcji domowego rutera. Niestety, pod względem funkcjonalnym rozwiązanie to ustępuje Filtrowi rodzinnemu. Dowiedzmy się, jak udostępnić dziecku bezpieczny internet.

1 Aby nasz system miał Filtr rodzinny, instalujemy pakiet Windows Live Essentials 2012. Instalujemy go z płyty dołączonej do biblioteczki CD-KOD: 020 lub KŚ+. Po uruchomieniu instalatora klikamy na Wybierz programy, które chcesz zainstalować.

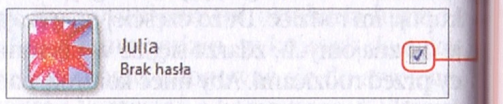
2 Zaznaczamy tylko opcję Bezpieczeństwo rodzinne i klikamy na Zainstaluj.



3 Uruchamiamy konfigurację Filtru rodzinnego, klikając na Wszystkie programy i na Bezpieczeństwo rodzinne usługi.

4 Usługa wymaga posiadania konta w serwisie Microsoft. Jeżeli go nie mamy, klikamy na Utwórz nowe konto, aby go utworzyć. Jeśli mamy konto, wpisujemy login oraz hasło i klikamy na Zaloguj.

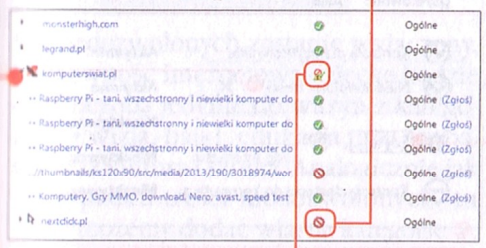
5 Następnie wybieramy użytkowników, których konta chcemy monitorować, i klikamy na Zapisz, następnie na Zamknij.



6 Nasze dziecko jest już chronione Filtrem rodzinnym. Aby dostosować ustawienia filtra i monitorować dziecko, otwieramy stronę **familysafety.microsoft.com** i logujemy się do naszego konta, używając tych samych danych co w punkcie 4. Wykorzystanie serwisu on-line do monitorowania dziecka ma olbrzymią zaletę – możemy z dowolnego miejsca i urządzenia sprawdzać, do czego wykorzystują komputer nasze dzieci.

7 Po zalogowaniu się do panelu ustawień zobaczymy listę użytkowników, których chcemy kontrolować, i dodanych komputerów. Klikamy na konto naszego dziecka.

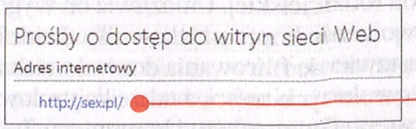
8 Klikamy na Raportowanie aktywn... i na Aktywność w sieci ... . Przejdziemy do raportu zawierającego wszystkie odwiedzane przez nasze dziecko strony internetowe. Obok adresów znajdziemy kategorię, do jakiej filtr przypisał dany serwis WWW, oraz akcję, jaka została podjęta. Witryny, które od razu zakwalifikowane były jako niebezpieczne, zostały całe zablokowane – świadczy o tym piktogram.



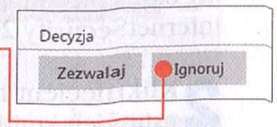
9 Jeżeli na stronie tylko niektóre elementy mogą być potencjalnie niebezpieczne, filtr tylko je blokuje. Strony takie mają oznaczenie. Warto wtedy rozwinąć adres i dokładnie sprawdzić, które elementy zostały zablokowane.

10 Jeżeli uznamy, że dana strona jest bezpieczna, możemy ją odblokować – klikamy wtedy na Zezwalaj. Analogicznie możemy zablokować witryny, które filtr uznał za bezpieczne, wtedy klikamy na przycisk Zablokuj.

11 Podczas przeglądania stron dziecko zostanie poinformowane, że witryna zawiera nieodpowiednie treści i musi poprosić rodzica o dostęp. Aby sprawdzić prośby dziecka, klikamy na Prośby.



12 Na liście przesłanych próśb o umożliwienie dostępu do strony znajdziemy adres internetowy, kategorię oraz datę i godzinę wysłania prośby. Jako osoba nadzorująca aktywność dziecka przy komputerze możemy podjąć decyzję – do wyboru mamy zignorowanie prośby lub zezwolenie na dostęp do tej strony.



13 Warto jeszcze czasem sprawdzać, co dziecko robi na komputerze, nie korzystając z internetu. Listę uruchamianych aplikacji sprawdzimy, klikając na Raportowanie aktywn... i na Aktywność na komp.

FUNKCJE W RUTERZE

Każdy ruter ma funkcję kontroli rodzicielskiej. Aby z niej skorzystać, musimy zalogować się do panelu administracyjnego. Tam skonfigurujemy harmonogram dostępu do internetu dla konkretnych urządzeń i blokadę wybranych stron, a czasem i treści. Funkcjonalność tego rozwiązania jest jednak mniejsza niż Filtru rodzinnego.

Więcej na: www.ebook4all.pl

Kontrola rodzicielska w G Data InternetSecurity 2014

Pakiet zabezpieczający komputer, z którego Czytelnicy mogą korzystać za darmo przez trzy miesiące (szczegóły na stronach 100–101), wyposażony jest w moduł kontroli rodzicielskiej. Umożliwia on wygodne stworzenie konta użytkownika dla dziecka i ustawienie filtrowania dozwolonych i niedozwolonych treści, a także kontrolowanie dostępu do internetu i komputera. Zobaczmy, jak używać tych funkcji.

Tworzenie konta użytkownika dla dziecka

1 Klikając podwójnie na ikonę w zasobniku systemowym, wywołujemy okno programu G Data InternetSecurity 2014.

2 Kliknięciem na otwieramy okno ustawień kontroli rodzicielskiej.

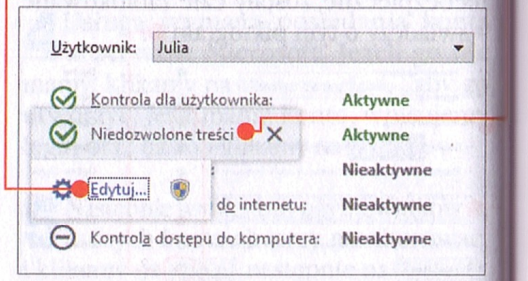
3 Żeby dodać nowe konto użytkownika dla dziecka, klikamy na przycisk Nowy użytkownik... w prawym dolnym rogu okna programu.

4 W nowym oknie w pole wpisujemy nazwę użytkownika, a w pola poniżej hasło, którego dziecko będzie używało do logowania się do Windows. Zmiany zatwierdzamy, klikając na Dodaj. Tak utworzone konto zostanie zapisane w ustawieniach Windows, a tym samym będzie dostępne w oknie logowania do systemu wyświetlanym przy starcie komputera.

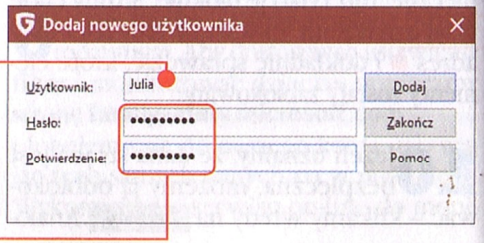
Ustawienia Kontroli rodzicielskiej

Domyślnie po utworzeniu konta dla dziecka funkcja kontroli rodzicielskiej jest aktywna. Włączony jest także domyślny filtr niedozwolonych treści. Dowiedzmy się, jak skonfigurować tę i pozostałe funkcje chroniące najmłodszych.

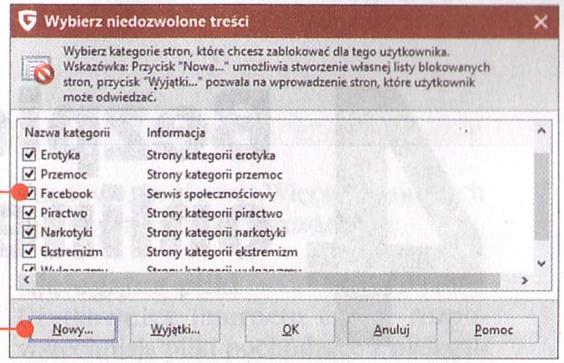
1 Klikamy na – rozwinie się menu, w którym klikamy na .



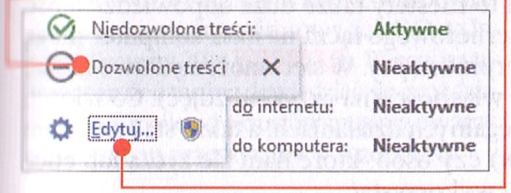
2 Otworzy się nowe okno. Widzimy w nim domyślne ustawienia, z których

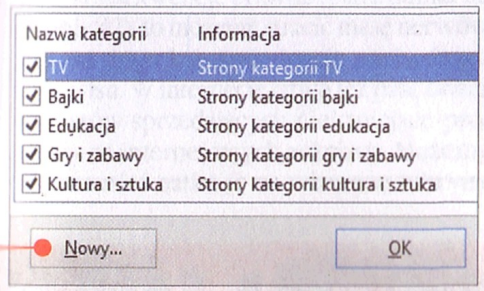


wynika, że blokowane są serwisy i treści związane z erotyką, przemocą, piractwem, narkotykami, ekstremizmem i wulgaryzmami. Jeśli nie chcemy, aby dziecko korzystało na przykład z serwisów społecznościowych , możemy dodać nową kategorię, klikając na . W nowym oknie wprowadzamy nazwę oraz opis i klikamy na przycisk OK. W kolejnym kroku podajemy adresy stron WWW lub słowa kluczowe, które mają być blokowane.



3 Filtr niedozwolonych treści blokuje wyłącznie określoną przez nas tematykę. Wszystkie pozostałe witryny dziecko będzie mogło oglądać. Inaczej będzie, jeśli klikniemy na i na . Wówczas filtr treści niedozwolonych zostanie wyłączony, a aktywność internetowa dziecka będzie ograniczona jedynie do witryn z kategorii telewizja, bajki, edukacja, gry i zabawy oraz kultura i sztuka. Analogicznie jak w wypadku treści niedozwolonych, tu także możemy dodać własną kategorię , poszerzając zakres uprawnień dziecka.

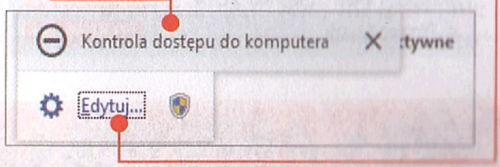




4 Funkcja Kontrola dostępu do internetu: pozwala na określenie, w które dni tygodnia, przez jaki czas dziecko będzie mogło korzystać z internetu. Odpowiednie wartości wybieramy za pomocą suwaków ,

a dokładne godziny, w których dostęp do globalnej sieci będzie aktywny, wybieramy po kliknięciu na przycisk .

5 Tak samo jak w wypadku kontroli dostępu do internetu, możemy określić przez ile godzin dziennie i w jakich porach dziecko może w ogóle używać komputera. Poza wyznaczonymi przez nas okresami nasza pociecha nie będzie w stanie zalogować się na swoje konto w Windows. Funkcję aktywujemy, klikając na i na .



Więcej na: www.ebook4all.pl

4 Bezpiecznie online

W internecie czyha na nas wiele niebezpieczeństw. Na jakie zagrożenia możemy natrafić i jak przed nimi się uchronić?

Dostęp do internetu to dziś konieczność – bez tego trudno uzyskać potrzebne informacje, zdobywać i utrzymywać znajomości czy wykonywać pracę. Internet to również nasze centrum rozrywki, a także sposób na wygodne zakupy bez wychodzenia z domu. Dostęp do światowej sieci to niestety także duża odpowiedzialność i różne zagrożenia. Za pośrednictwem internetowego łącza na nasz komputer mogą przedostać się szkodniki i włamać się cyberprzestępcy. W sieci możemy łatwo zostać oszukani czy okradzeni z naszej cyfrowej własności (na przykład zdjęć). Co więcej, nieświadomie możemy wziąć udział w nielegalnych działaniach, a także stać się celem internetowych stalkerów (prześladowców) czy osób, które nam źle życzą lub chcą nas i naszych bliskich (na przykład dzieci) wykorzystać.

W tym rozdziale przeczytamy o czyhających na nas w internecie zagrożeniach oraz dowiemy się, jak ich uniknąć. Poznamy zasady bezpiecznego korzystania z różnych internetowych usług i unikania kłopotów, a także dowiemy się, jak zabezpieczać naszą cyfrową własność przed kradzieżą i rozpowszechnieniem i co robić w razie naruszenia naszej prywatności. **kż**

DROGOWSKAZ

- Zagrożenia w sieci s. 39
- Korzystanie z usług w internecie s. 41
- Publikowanie treści w internecie s. 42
- Śledzenie naszych działań s. 44

PRZYDATNE PROGRAMY

- G Data InternetSecurity 2014 CD-KOD: 007
- Picture-Shark TYLKO W KS+

Zagrożenia w sieci

Internet to nie tylko zabawa i świetne źródło informacji. Zobaczmy, na jakie zagrożenia możemy natknąć się w sieci.

Szkodniki i szpiedzy

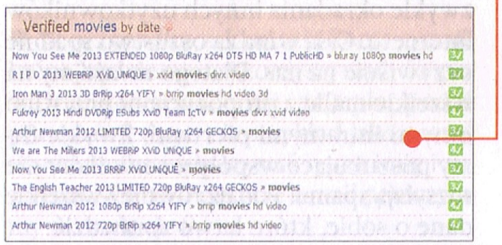
Obecne w internecie szkodniki (wirusy, trojany, rootkity) mogą przedostać się na nasz komputer, zniszczyć naszą pracę, narobić bałaganu i wykraść ważne dane. Poprzez e-maile, do złudzenia przypominające te od znanych nam instytucji (phishing), a także za pośrednictwem oprogramowania szpiegującego (spyware, keyloggery) cyberprzestępcy wyłudzają loginy i hasła. Przed szkodliwym oprogramowaniem ochroni nas dobry program antywirusowy (jak G Data InternetSecurity 2014 TYLKO W KS+). Więcej na temat zagrożeń można dowiedzieć się z rozdziału 1. Na e-maile od oszustów musimy uważać sami – o tym przeczytamy w rozdziale 8.

Portale i osoby wyłudzające pieniądze

Niektóre serwisy mają bezprawne zapisy w regulaminach, na podstawie których nakładają różnego rodzaju opłaty za korzystanie ze swoich usług. Przykładem takich portali może być Pobieraczek.pl lub Plikostrada.pl. Choć ich działania są nielegalne i nie grożą nam konsekwencje prawne (patrz ramka na stronie 42), to możemy stracić masę nerwów nękani przez korespondencję pochodzącą z serwisu. W internecie łatwo też paść ofiarą oszustów sprzedających nieistniejące produkty na internetowych aukcjach. Możemy się również natknąć na udawane witryny sklepowe, bankowe. Więcej o zakupach w sieci przeczytamy w rozdziale 6.

Nielegalne pliki

Użytkownicy internetu często rozpowszechniają pliki pochodzące z nielegalnych źródeł (programy, pliki z muzyką czy filmami). Takie pliki mogą być zainfekowane, a także przysporzyć nam kłopotów z prawem. Jeśli korzystamy z sieci p2p, to pobierając dany plik, jednocześnie udostępniamy go innym użytkownikom. A to oznacza, że go nielegalnie rozpowszechniamy – za to możemy być pociągnięci do odpowiedzialności karnej. Starajmy się pobierać pliki tylko z legalnych, zaufanych źródeł, na przykład stron producentów oprogramowania.



Nieznajomi w sieci

Internet pozwala być anonimowym, a to oznacza, że nigdy nie mamy pewności, kto z nami rozmawia po drugiej stronie łącza. Użytkownicy internetu mogą udawać naszych przyjaciół i wyciągać informacje o naszym prywatnym życiu, aby następnie wykorzystać je do nękania czy szantażu.

Eksperci G Data ostrzegają!
System Android jest głównym celem a ów na urządzenia mobilne.

Więcej na: www.ebook4all.pl

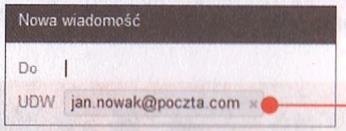
Dlatego zawsze stosujmy zasadę ograniczonego zaufania wobec nieznajomych.

Złodzieje tożsamości

Kradzież tożsamości to zagrożenie, które dotyczy nieuważnych i łatwowiernych użytkowników internetu. Zwykle sami udostępniamy informacje o sobie, wierząc, że dostaliśmy na przykład intratną ofertę pracy. Tymczasem jest to tylko przykrywka, a złodziej wykorzystuje naszą tożsamość do swoich niecnych celów, zwykle okradania innych użytkowników internetu. Cała wina za oszustwo spadnie oczywiście na nas. Dlatego uważajmy na wszelkie maile z propozycjami pracy lub innymi intratnymi ofertami. Zwykle firmy poszukujące współpracowników nie rozsyłają spamu. Podają również wszelkie dane o sobie, które łatwo sprawdzić.

Łańcuszki i spam

Łańcuszki to najczęściej maile z prośbą o przesyłanie dalej jak największej liczbie znajomych. W treści łańcuszka znajdują się albo nieprawdziwe, albo nieaktualne informacje, a sama wiadomość to tak naprawdę spam. Łańcuszek ma zwykle na celu zapchanie łączy internetowych, a także przechwycenie jak najwięcej adresów e-mailowych. Możliwe jest również rozsiewanie tą drogą szkodników. Dlatego, jeśli otrzymamy taką wiadomość, najlepiej od razu ją skasować. Przy okazji warto zapamiętać, aby wysyłając e-mail do większej liczby znajomych, wpisać ich adresy w polu UDW (ukryta kopia).



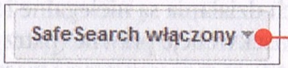
Złodzieje własności intelektualnej

Internet to idealne miejsce na prezentację naszej twórczości, na przykład zdjęć. Jednak i tutaj czyha na nas zagrożenie w postaci złodziei. Skradzione zdjęcie może być na przykład twórczo wykorzystane w czyimś projekcie albo stać się celem pośmiewiska na innych witrynach. Jak się przed tym chronić, przeczytamy na stronie 43.

modelka: Dorota Kuna, fot. Alicja Żebruń

Pornografia i przemoc

Obrazy pełne przemocy i treści pornograficznych mogą zaszkodzić szczególnie najmłodszym. Łatwy dostęp do tego typu zawartości powoduje, że ciężko się przed tym uchronić. Możemy jednak próbować. Jak? Na przykład włączając filtr treści o charakterze seksualnym w wyszukiwarce internetowej. Więcej na temat ochrony dzieci przeczytamy w rozdziale 3.



Uzależnienie od internetu

Od wszystkiego, co przyjemne, można się uzależnić, także od internetu. Jednak każde uzależnienie niesie za sobą zagrożenia. W przypadku internetu to zwykle niezdrowy tryb życia i niepotrzebne tracenie czasu, który można wykorzystać bardziej produktywnie.

Korzystanie z usług w internecie

Każdy serwis czy usługa w internecie może mieć inne wymagania. Choć zasady bezpiecznego korzystania z internetu są uniwersalne, w przypadku każdej z usług należy stosować zasady ukierunkowane na specyfikę usługi.

Podawanie danych

Musimy ostrożnie udostępniać swoje prawdziwe dane, jednak w niektórych przypadkach jest to konieczne.

- Rejestrując się na stronie internetowego sklepu, warto od razu podać nasze prawdziwe dane. Będą one potem potrzebne do wysyłki towaru czy w razie reklamacji zakupionego produktu. Więcej o bezpiecznych zakupach online przeczytamy w rozdziale 6.

- Dokładnych danych nie musimy podawać w przypadku usług, które nie potrzebują tych informacji do poprawnego funkcjonowania i współpracy z nami. Szczególnie gdy korzystamy z serwisu o nie najlepszej opinii (patrz strona 39).

- W celu skorzystania z niektórych usług warto założyć osobną skrzynkę e-mail. Nie będziemy zaśmiecać naszej głównej skrzynki pocztowej ewentualnym spamem.

- W przypadku zakładania konta e-mail, które będziemy wykorzystywać do poważnej korespondencji, najlepiej podać prawdziwe dane, na przykład jako nazwę użytkownika wykorzystać nasze imię i nazwisko. Więcej o poczcie e-mail przeczytamy w rozdziale 8.

Bezpieczne hasło

Podczas tworzenia konta pamiętajmy o zadbaniu o dobre hasło – trudne do złamania, a łatwe do zapamiętania przez nas.

CO O NAS WIE DOSTAWCA INTERNETU

Dostawca internetu może teoretycznie gromadzić wszelkie informacje dotyczące ruchu sieciowego, jaki generuje nasz komputer, a także jego zawartości. W praktyce są to dane dotyczące adresu odwiedzanych stron, ilości przesłanych danych, czasu aktywności. Te dane ustawowo należy gromadzić i przechowywać przez okres od 6 miesięcy do 2 lat. Dostęp do nich może uzyskać policja i prokuratura, a w trakcie postępowania sądowego również uczestnicy sporu. Z kolei w przypadku danych osobowych ustawa o ich ochronie nie definiuje jednoznacznie okresu, w jakim muszą być usunięte. Tłumaczone jest to bardzo ogólnikowo: „Nie dłużej, niż to jest konieczne do osiągnięcia celu przetwarzania". Na przetwarzanie musimy wyrazić zgodę, a dostawca musi uzasadnić, dlaczego jest to konieczne. Mamy prawo wglądu do dotyczących nas danych, jednak tylko, gdy ich ujawnienie nie narusza interesów osób trzecich lub bezpieczeństwa kraju, a także nie częściej niż raz w ciągu 6 miesięcy.

Więcej na: www.ebook4all.pl

NIEDOZWOLONE ZAPISY W REGULAMINACH

Regulaminy usługodawców pełne są różnych zapisów i postanowień. Niektóre z nich są niedozwolone, jak na przykład zapis: „Wszelkie zmiany Regulaminu wchodzą w życie z dniem ich opublikowania na stronie [...]„ czy „Regulamin może zostać zmieniony w dowolnym momencie". Warto zapoznać się z listą niedozwolonych zapisów opublikowaną na stronie UOKiK pod adresem **www.uokik.gov.pl/niedozwolone_klauzule.php**. Na temat niedozwolonych zapisów w regulaminach dotyczących zakupów online przeczytamy w rozdziale 6.

Ułożenie odpowiedniego hasła nie jest trywialne. Istnieją jednak triki, które nam w tym pomogą. O tym, jak tworzyć bezpieczne hasła, dowiemy się z rozdziału 9.

Czytajmy regulaminy

Zakładając konto w danej usłudze, zgadzamy się na zapisy regulaminów. Nie wszystko musi nam się podobać i choć zapisy niektórych regulaminów można podważyć (patrz ramka), to lepiej dmuchać na zimne. Jeśli jakiś zapis nie wzbudza naszego zaufania, nie rejestrujmy się na tej stronie. Warto jednak wiedzieć, że za pewnymi zapisami w regulaminach nie zawsze stoją niecne zamiary właścicieli portalu. Na przykład portale społecznościowe wymagają zgody na wykorzystywanie naszych treści do normalnego funkcjonowania. Bo jak bez naszej zgody Facebook mógłby pokazywać innym użytkownikom portalu nasz wizerunek w dowolnym miejscu na świecie?

Publikowanie treści w internecie

Internet służy nie tylko do przeglądania stron i szukania informacji bądź robienia zakupów. Pozwala również publikować wszelkiego rodzaju treści, takie jak komentarze, wpisy blogowe czy zdjęcia lub filmy. Zobaczmy, czego nie publikować w sieci oraz jak zabezpieczyć własne treści.

Czego nie publikować w sieci

Niektórych treści lepiej nie publikować w internecie, szczególnie w miejscach publicznych, do których każdy ma dostęp. Jakie to treści?

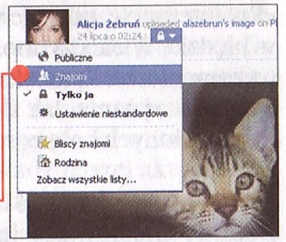
- Informacje o naszym prywatnym życiu, prywatne dane kontaktowe czy inne dane, które mogą wykorzystać złodzieje lub inne osoby, które nam źle życzą.
- Bardzo prywatne czy intymne zdjęcia, a także fotografie, które mogą źle o nas świadczyć lub wystawić nas na pośmiewisko (w internecie łatwo rozpowszechnić zdjęcia).
- Wpisy, które mogą kogoś urazić (pamiętajmy o netykiecie), a także treści niezgodne z prawem oraz utwory (na przykład zdjęcia) niebędące naszą własnością lub gdy nie mamy zgody na publikację fotki czy widniejącego na niej wizerunku.

Jak zabezpieczyć publikowane treści

Treści publikowane w internecie warto zabezpieczyć na różne sposoby, aby nie padły łupem cyberzłodzieja.

- Fotografie warto oznaczyć znakiem wodnym (na przykład za pomocą darmowego programu Picture-Shark TYLKO W KS+). Nie zagwarantuje to wprawdzie, że zdjęcie nie zostanie skopiowane, ale może działać odstraszająco na potencjalnych złodziei. A także informować innych internautów o źródle pochodzenia obrazu.

- Jeśli prowadzimy stronę czy blog, w stopce umieśćmy informację o zastrzeżonych prawach do treści publikowanych na stronie (na przykład w postaci: Copyright © Autor 2013. Wszelkie prawa zastrzeżone). Choć według obowiązujących przepisów nasze treści i tak są chronione, lepiej jednak poinformować o tym odwiedzających naszą witrynę.
- Dostęp do galerii czy naszego konta społecznościowego ustawiamy jako prywatny (tylko dla znajomych lub zaufanych osób, którym przekażemy link do zdjęć).



- Treści (na przykład pliki lub archiwa) umieszczane w chmurze warto zaszyfrować. W tym celu możemy skorzystać z takich narzędzi, jak SecretSync, TrueCrypt czy Boxcryptor. Wieloplatformowy Boxcryptor stosuje algorytmy szyfrujące AES-256 oraz RSA. Obsługuje wszystkie najważniejsze chmury, w tym Dropbox, Box.net czy Sugarbox. Zaszyfrowane dane można udostępnić wskazanym użytkownikom pod warunkiem, że zainstalują one Boxcryptora.

NARUSZONA PRYWATNOŚĆ – CO ROBIĆ

Nawet gdy zadbamy o anonimowość oraz publikowane treści, zawsze się może zdarzyć, że ktoś ze znajomych naruszy naszą prywatność, publikując (nawet bez złych zamiarów) nasze zdjęcia czy inne dane. Jeśli prośba do znajomego o usunięcie treści nie zadziała, musimy skontaktować się z webmasterem strony, na której są opublikowane nasze prywatne informacje (patrz strona 70). W świetle prawa administrator ma obowiązek niezwłocznego usunięcia nielegalnych bądź obraźliwych treści. Warto jednak wiedzieć, że z wyników wyszukiwania Google i innych wyszukiwarek zindeksowane dane nie znikną od razu. Trzeba trochę poczekać albo zawiadomić Google poprzez odpowiedni formularz. Więcej informacji znajdziemy na stronie **https://support.google.com/webmasters/answer/1663688**.

Więcej na: www.ebook4all.pl

Śledzenie naszych działań

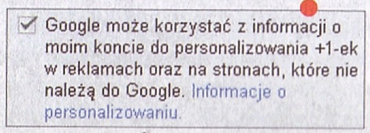
Jeśli wydaje nam się, że tego, co robimy w internecie, nikt nie widzi, to jesteśmy w błędzie. Wiele czynności zostawia ślady na komputerze. Są też skrypty, które śledzą nasze poczynania. Jak stać się niewidocznym dla innych i nie zostawiać śladów?

Anonimowe korzystanie z sieci

Jeśli nie chcemy, aby inni użytkownicy sieci widzieli, co publikujemy, a także gdzie znajduje się nasz komputer, warto skorzystać z protokołów zabezpieczeń i sieci pozwalających na anonimowe surfowanie, takich jak na przykład Tor (patrz strona 72). Więcej o tym można przeczytać w rozdziale 7, z którego dowiemy się także o ustawieniach prywatności w sieciach społecznościowych i surfowaniu bez zostawiania śladów na komputerze.

Personalizacja usług

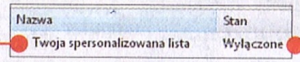
Wiele serwisów chce korzystać z naszych treści w celu tak zwanej personalizacji usług (to oznacza, że na przykład będziemy zasypywani reklamami dostosowanymi do tematyki, którą poruszamy, komunikując się za pomocą danej usługi). By serwis nie korzystał z informacji o nas, trzeba zmienić ustawienia prywatności. Czasem możliwe jest to już na etapie zakładania konta, jak w przypadku usługi Google+.



Blokowanie skryptów śledzących

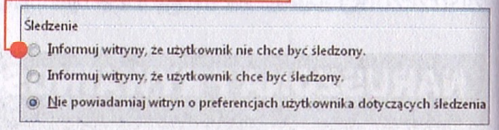
Skryptom śledzącym zawdzięczamy spersonalizowane wersje stron WWW, a dostawcy internetu – statystyki użytkowania sieci. Niestety, tego typu skrypty mogą naruszać naszą prywatność i sprowadzać zagrożenia na komputer. Aby się chronić przed inwigilacją, aktywujmy funkcję DoNotTrack (nie śledź), którą stosują najpopularniejsze przeglądarki.

■ W przeglądarce **Internet Explorer 9** i **10** klikamy na przycisk ⚙, następnie na Bezpieczeństwo i Ochrona przed śledzeniem... Klikamy dwukrotnie na pole i zaznaczamy Blokuj automatycznie, a potem klikamy na OK. Teraz z menu kontekstowego dla

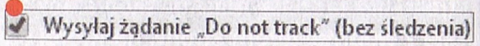


wybieramy Włącz. Aktywowaliśmy funkcję DoNotTrack.

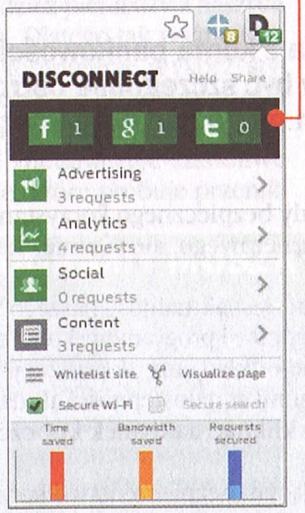
■ W Mozilla **Firefox** klikamy na Firefox, wybieramy Opcje i Opcje. Na zakładce zaznaczamy pole, by blokować śledzenie. Klikamy na OK.



■ W **Google Chrome** klikamy na przycisk ☰, a następnie wybieramy Ustawienia i Pokaż ustawienia zaawansowane... W sekcji Prywatność zaznaczamy pole wyboru. Klikamy na OK.



■ Sama funkcja DoNotTrack nie gwarantuje pełnej blokady, można zatem posłużyć się dodatkiem do przeglądarki **Disconnect**. Po zainstalowaniu dodatek doda ikonę D. do paska adresowego. Po wejściu na daną witrynę klikamy na tę ikonę, by wyświetlić okienko z podsumowaniem aktywnych i blokowanych skryptów śledzących. Ikony symbolizujące skrypty są interaktywne – wystarczy na nie kliknąć, by nimi zarządzać.

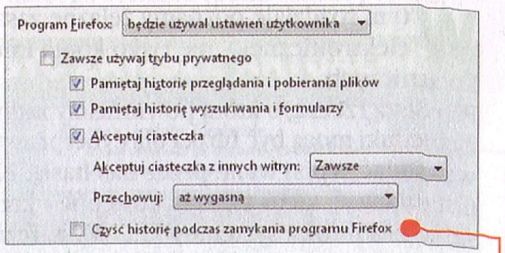


■ Bardzo popularnym dodatkiem, niestety jedynie dla Firefoksa, jest **NoScript**. Jego zadanie to blokowanie wszystkich, także szkodliwych, skryptów JavaScript i apletów Java.

Ukrywanie danych przed innymi użytkownikami

Nasza aktywność podczas przeglądania internetu jest szczegółowo zapamiętywana przez przeglądarki internetowe. W domu te funkcje mogą poprawić komfort surfowania, ale w nieznanym miejscu wystawiają naszą prywatność na publiczny widok. Najpewniejszą opcją jest stosowanie przenośnych wersji przeglądarek i innych narzędzi sieciowych uruchamianych z pendrive'a. Jeśli zmuszeni jesteśmy do korzystania z przeglądarki w kafejce, kasujmy wszelkie ślady naszej aktywności.

■ Wszelkie sugestie, by zapamiętać hasło i inne wprowadzane dane, ignorujmy.



■ Historia, hasła, ciasteczka, dane formularzy identyfikują naszą aktywność. Możemy dostosować reguły ich zapamiętywania lub wymusić kasowanie. Dla Firefoksa te opcje znajdziemy na zakładce . Możemy też włączyć tryb prywatny (strona 72).

INWIGILACJA PRISM – JAK SIĘ BRONIĆ

PRISM (program amerykańskiej Agencji Bezpieczeństwa Narodowego) pozwala na niczym nieskrępowany dostęp do praktycznie wszystkich informacji o naszej sieciowej aktywności oraz do tworzonych przez nas cyfrowych treści. Wszystkie najważniejsze usługi internetowe, systemy i zamknięte oprogramowanie mogą współpracować z PRISM. Nawet gdy zapewniani jesteśmy o bezpieczeństwie naszych danych osobowych, ryzyko naruszenia prywatności zawsze istnieje. Ochrona przed wpływem PRISM wymaga dużej dyscypliny, ale jest możliwa. Wiąże się ze zmianą podejrzanych aplikacji na bezpieczne. Pomocna w tym celu jest strona **prism-break.org** z listą darmowych odpowiedników najważniejszego oprogramowania.

Więcej na: www.ebook4all.pl

5 Bezpieczny e-bank

Podczas korzystania z konta bankowości elektronicznej powinniśmy być szczególnie ostrożni. Luki w zabezpieczeniach mogą nas dużo kosztować

W tym rozdziale poznamy żelazne zasady bezpiecznego korzystania z bankowości elektronicznej – nie tylko konta internetowego, ale również kart kredytowych i płatniczych.

Pierwszą rzeczą, o którą powinniśmy zadbać, jest aktualność naszego Windows. Niezałatane luki mogą być furtką dla cyberprzestępców i programów, które mogą na przykład wykradać wpisywane przez nas hasła. Nie odkładajmy aktualizacji Windows, tylko instalujmy je, kiedy tylko są dostępne – komunikat o dostępności aktualizacji wyświetla się w zasobniku systemowym. Wystarczy kliknąć na dymek i poczekać kilka minut na zainstalowanie **updatów***.

Niezwykle ważnym czynnikiem poprawiającym bezpieczeństwo korzystania z bankowości elektronicznej na komputerze jest aktualny, dobry program zabezpieczający, na przykład pakiet G Data InternetSecurity 2014. Składniki takiego oprogramowania, jak antywirus, firewall czy moduł **antyspyware***, zabezpieczają nas przed groźnym oprogramowaniem.

Jeśli komputer jest odpowiednio zabezpieczony, należy wyeliminować tak zwany czynnik ludzki, czyli ustawić odpowiednio bezpieczne, unikatowe hasło (więcej o hasłach w rozdziale 9), nie korzystać z konta na niezabezpieczonych komputerach i rozpoznawać próby phishingu (więcej o phishingu w rozdziale 8). **pg**

* Wyjaśnienie pojęcia w leksykonie na stronach 102–103

DROGOWSKAZ

- Bezpieczny komputer to podstawa s. 47
- Podstawowe środki bezpieczeństwa s. 48
- Jak rozpoznać phishing bankowy s. 49
- Bezpieczne płatności internetowe s. 51
- Zagrożenia związane z kartami s. 52
- Zagrożenie czai się w skrzynce s. 53

PRZYDATNE PROGRAMY

- G Data InternetSecurity 2014 CD-KOD: 007

Bezpieczny komputer to podstawa

Czasy złośliwych wirusów kasujących pliki na dysku już dawno minęły. Teraz przestępcy tworzą oprogramowanie szpiegowskie, które wykrada ważne dane i pozwala na kradzież pieniędzy z naszych kont bankowych. Dlatego tak ważne jest, aby na każdym komputerze wykorzystywanym do łączenia się ze stroną banku był zainstalowany pakiet zabezpieczający, który wykryje i zneutralizuje szkodliwe oprogramowanie, które próbuje przeniknąć do systemu. Po zainstalowaniu antywirusa powinniśmy przeskanować dysk w poszukiwaniu szkodliwych programów, które mogą między innymi rejestrować wpisywane przez nas loginy i hasła.

Więcej o zabezpieczaniu komputera przeczytamy w rozdziale 1.

Bardzo ważne jest również aktualizowanie programów, których używamy na co dzień, oraz aplikacji będących składnikami naszego systemu (patrz ramka poniżej).

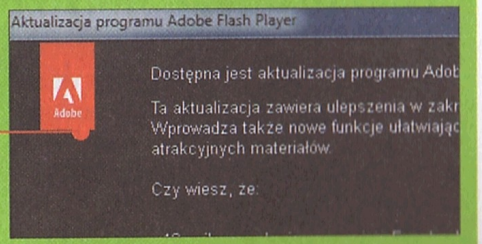
JAKIE PROGRAMY MUSZĄ BYĆ ZAWSZE AKTUALNE

System i programy

Niechlubnymi liderami pod względem liczby wykrywanych luk są: **Adobe Reader**, **Adobe Flash Player**, oprogramowanie **Java**, **Internet Explorer** i **Windows**. To oprogramowanie jest zainstalowane na większości komputerów i dlatego jest łakomym kąskiem dla cyberprzestępców. Kiedy więc pojawia się dymek informujący o dostępnej aktualizacji, czy to dotyczący systemu Windows, Adobe Flash Playera czy Javy, niezwłocznie klikamy na niego i postępując zgodnie ze wskazówkami na ekranie, instalujemy aktualizację.

Przeglądarka

Zaktualizowana przeglądarka, którą wykorzystujemy podczas korzystania ze strony banku, to podstawa. Jeśli nasza przeglądarka nie aktualizuje się automatycznie i pojawi się komunikat o dostępnej aktualizacji, wykonajmy ją jak najszybciej.



Eksperci G Data ostrzegają!
W najbliższych 6 miesiącach możemy spodziewać się potrojenia liczby zagrożeń na system Android.

Więcej na: www.ebook4all.pl

Podstawowe środki bezpieczeństwa

Aby być szczęśliwym i bezpiecznym użytkownikiem bankowości elektronicznej, należy przestrzegać kilku prostych zasad. Oto one.

Bezpieczne hasło

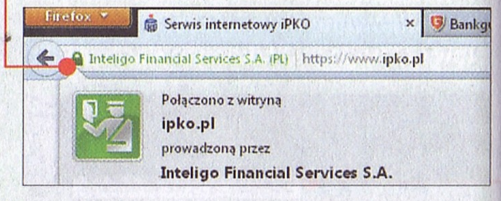
O tworzeniu bezpiecznych haseł przeczytamy w rozdziale 9. Ważne, aby hasło do internetowego rachunku bankowego było inne niż jakiekolwiek używane przez nas na komputerze.
Hasła do konta internetowego oczywiście nikomu nie zdradzamy, pod żadnym pozorem nigdzie nie zapisujemy, a podczas wpisywania zwracamy uwagę, czy nikt zza pleców nie patrzy nam na ręce.

Bezpieczny komputer i sieć

Ze swojego konta internetowego korzystamy tylko na komputerach, których wysokiego poziomu zabezpieczeń jesteśmy pewni. Pod żadnym pozorem nie logujemy się na stronę banku na przypadkowych pecetach.
Aby zabezpieczyć się przed przechwyceniem danych logowania (loginu, hasła, kodów jednorazowych) przez przestępców, nie logujemy się na stronę banku w otwartych sieciach bezprzewodowych. Działający w galerii handlowej, w kawiarni czy w innym miejscu **hotspot*** może być przejęty przez cyberprzestępców lub po prostu podstawiony.

Certyfikat bezpieczeństwa

Zanim zalogujemy się na stronę banku, sprawdzamy jej certyfikat bezpieczeństwa. Zajmuje to krótką chwilę, a daje pewność, że strona nie jest fałszywa i nasze dane logowania nie lądują właśnie w bazie przestępcy. Aby sprawdzić certyfikat strony banku, którą otworzyliśmy, z lewej strony adresu, w zależności od używanej przeglądarki, klikamy na nazwę certyfikatu lub ikonę kłódki oznaczającą szyfrowane połączenie. Certyfikat powinien zawierać nazwę banku.



BANKGUARD CHRONI BANKOWOŚĆ

W pakiecie zabezpieczającym G Data InternetSecurity 2014 wbudowany jest moduł zwiększający bezpieczeństwo korzystania z bankowości internetowej – BankGuard. Zmiany dokonywane przez konie trojańskie stworzone do przechwytywania danych logowania czy podmiany strony banku na fałszywą mają miejsce w pamięci RAM. G Data BankGuard wykrywa próby infekcji i zastępuje zainfekowany obszar pamięci jego bezpieczną kopią. BankGuard pracuje w tle (oczywiście kiedy uruchomiony jest pakiet G Data) i w razie wykrycia infekcji usuwa zagrożenie. Jeśli konia trojańskiego nie da się usunąć, BankGuard wyświetla komunikat zalecający przerwanie wykonywania operacji bankowych na komputerze, aż do czasu usunięcia zagrożenia.

* Wyjaśnienie pojęcia w leksykonie na stronach 102–103

Jak rozpoznać phishing bankowy

Przestępcy stosują różne wymyślne techniki, aby uzyskać dostęp do naszych kont bankowych. Jedną z metod mających na celu wyłudzenie loginu i hasła do naszego rachunku internetowego jest phishing.

Amatorski phishing

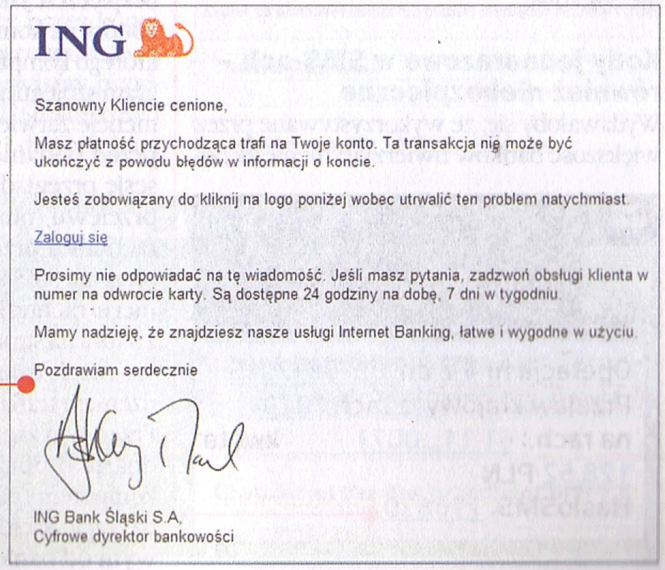
Zdarzają się również mniej wyszukane metody phishingu. Przestępca, podszywając się pod dział obsługi klienta banku, prosi po prostu odbiorcę e-maila o podanie loginu i hasła do rachunku internetowego pod pozorem dokonania czynności serwisowych. Pamiętajmy, żaden bank nigdy nie poprosi nas o podanie e-mailem ani inną drogą danych logowania do rachunku, i to w żadnym celu! Login i hasło wpisujemy tylko i wyłącznie na stronie banku w celu zalogowania się do rachunku.

Typowy phishing

W większości wypadków przestępcy wysyłają do przypadkowych odbiorców wiadomość spreparowaną tak, aby przypominała e-mail wysłany przez bank. Sfałszowane wiadomości są często łatwe do rozpoznania, bo zawierają tekst nieudolnie przetłumaczony automatycznym translatorem, na przykład . W treści wiadomości phishingowej, kuszeni niespodziewanym wpływem na konto lub ostrzegani przed zmyślonym niebezpieczeństwem, jesteśmy najczęściej namawiani na kliknięcie na link do strony banku i zalogowanie się na niej. Nie klikajmy nigdy na taki link! Spreparowana strona może instalować na komputerze oprogramowanie szpiegowskie. Natomiast nieostrożni użytkownicy, którzy podadzą na fałszywej stronie login i hasło do swojego konta, mogą stracić do niego dostęp lub nawet zostać okradzionym z pieniędzy zgromadzonych na rachunku.

Groźna lista kodów jednorazowych

Przestępcy używają również bardziej wyrafinowanych metod na kradzież pieniędzy z kont bankowych. Przedstawiona niżej metoda jest groźna dla osób, które korzystają z listy kodów jednorazowych (wydrukowanej czy w formie zdrapki). Kiedy wejdziemy na zainfekowaną stronę (zarażona może być nawet popularna strona, na którą codzien-


ING

Szanowny Kliencie cenione,

Masz płatność przychodząca trafi na Twoje konto. Ta transakcja nię może być ukończyć z powodu błędów w informacji o koncie.

Jesteś zobowiązany do kliknij na logo poniżej wobec utrwalić ten problem natychmiast.

Zaloguj się

Prosimy nie odpowiadać na tę wiadomość. Jeśli masz pytania, zadzwoń obsługi klienta w numer na odwrocie karty. Są dostępne 24 godziny na dobę, 7 dni w tygodniu.

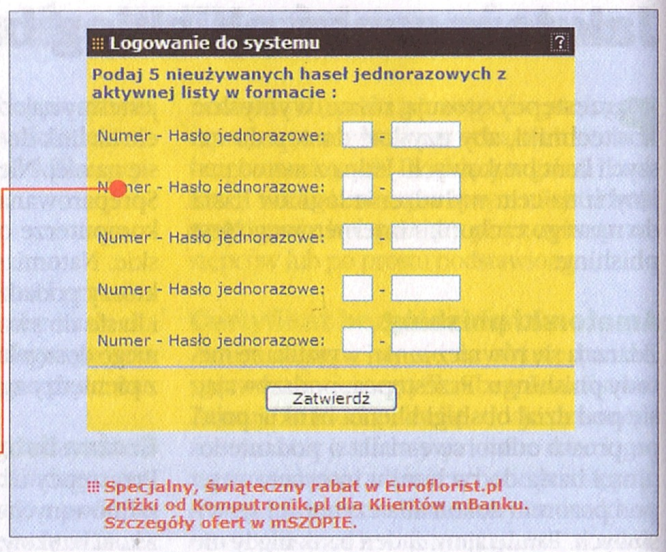
Mamy nadzieję, że znajdziesz nasze usługi Internet Banking, łatwe i wygodne w użyciu.

Pozdrawiam serdecznie

ING Bank Śląski S.A.
Cyfrowe dyrektor bankowości

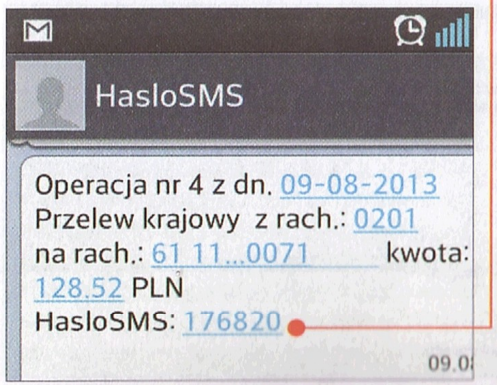
Więcej na: www.ebook4all.pl

nie wchodzą miliony internautów), szkodliwe oprogramowanie skanuje nasz komputer i wyszukuje luki w zabezpieczeniach, przez które dostaje się do systemu. W momencie kiedy logujemy się do banku i wpisujemy login i hasło, program szpiegowski już działa i przechwytuje dane logowania. W tym momencie wyświetla się sfałszowana strona z prośbą o podanie kilku haseł z listy haseł jednorazowych. Jeśli nieświadomy podstępu użytkownik poda kody jednorazowe na sfałszowanej stronie, przestępcy mają już wszystko, co potrzebne do wykonania dowolnej operacji na naszym koncie – zlecenie przelewu, ustawienie zlecenia stałego czy zmiana sposobu uwierzytelniania z listy haseł na potwierdzenie SMS-owe.



Kody jednorazowe w SMS-ach – również niebezpieczne

Wydawałoby się, że wykorzystywane przez większość banków uwierzytelnienie za pomocą kodów jednorazowych wysyłanych na telefon komórkowy jest bezpieczne. Faktycznie jest to dość bezpieczny sposób potwierdzania wykonania transakcji, ale przestępcy znaleźli sposób na ominięcie zabezpieczeń. Jak działa wyłudzanie z użyciem kodów na komórkę? Kiedy użytkownik, na którego komputerze jest zainstalowany program szpiegujący, wykonuje przelew, w momencie zatwierdzania operacji (ale jeszcze przed podaniem kodu) szpieg przejmuje sesję przeglądarki i podmienia parametry przelewu (numer konta i kwotę) na dane rachunku przestępcy. Kiedy użytkownik otrzyma SMS i niesprawdzając kwoty i numeru rachunku odbiorcy, przepisze kod z SMS-a na stronie banku (a tak niestety przeważnie się dzieje), pieniądze za jego potwierdzeniem trafiają na podstawione konto. Przed tym zagrożeniem można się ustrzec, dbając o poziom zabezpieczeń swojego komputera (patrz rozdział 1) oraz uważnie czytając każdy SMS z kodem jednorazowym od banku.



Bezpieczne płatności internetowe

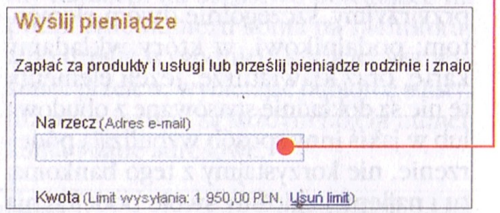
Zakupy w sieci są coraz popularniejsze wśród internautów. To wygodne rozwiązanie niesie jednak ze sobą pewne zagrożenia związane z płatnościami. Zagrożenie może przyjść z kilku kierunków, bo przecież za zakupy możemy płacić przelewem internetowym, szybkim przelewem realizowanym przez pośrednika, a za zagraniczne zakupy kartą kredytową czy za pośrednictwem systemu **PayPal***. Zobaczmy, na co zwrócić uwagę, aby nasze pieniądze trafiły do właściwego odbiorcy zamiast na konto przestępców.

Niebezpieczne płatności kartą

Płatności kartą kredytową nie są najbezpieczniejszym sposobem regulowania należności za zakupy i lepiej ich unikać. Kiedy płacimy kartą w internecie, podajemy jej numer, datę ważności i kod CVV/CCV2, czyli wszystkie dane, które są potrzebne do obciążenia karty przez kogokolwiek. Dodatkowym zagrożeniem są luki w zabezpieczeniach serwisów przyjmujących płatności kartami. Stosunkowo często zdarzają się wycieki danych kart kredytowych klientów różnych sklepów i usługodawców internetowych. Dane kart są następnie wystawiane na sprzedaż na przestępczych forach internetowych.

Płatność przez e-mail

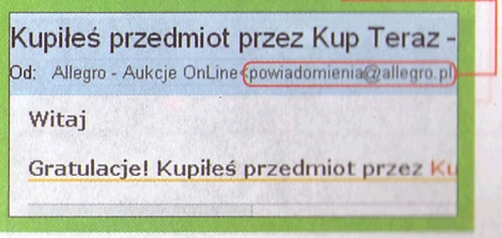
Jeżeli chcemy robić zakupy za granicą, lepiej załóżmy konto w serwisie PayPal. Aby płacić za zakupy za pośrednictwem PayPal, wystarczy założyć konto w serwisie **www.paypal.pl** i zasilić swoje konto przelewem na wybraną przez siebie kwotą. Płatności przez PayPal akceptuje większość zagranicznych sklepów internetowych i serwisów aukcyjnych, na przykład eBay. Aby przelać pieniądze innemu użytkownikowi PayPal, na przykład sprzedawcy, wystarczy wpisać adres e-mail, pod którym jest zarejestrowany w PayPal.



OSZUSTWO PO WYGRANEJ AUKCJI

Znane są przypadki, kiedy użytkownicy popularnych serwisów aukcyjnych po wygraniu aukcji albo tuż przed jej zakończeniem otrzymywali sfałszowany e-mail (z numerem konta przestępcy) od osoby podszywającej się pod sprzedawcę. Pamiętajmy, że potwierdzenie wygrania aukcji jest wysyłane przez automat serwisu, a nie osobiście przez sprzedawcę.

Na przykład po wygraniu aukcji na Allegro otrzymujemy e-mail z adresu.



* Wyjaśnienie pojęcia w leksykonie na stronach 102–103

Więcej na: www.ebook4all.pl

Zagrożenia związane z kartami

Na poprzedniej stronie dowiedzieliśmy się, jakie zagrożenia niosą ze sobą płatności przez internet kartą kredytową. To jednak niejedyne zagrożenia związane z kartami bankowymi. Niestety, pieniądze możemy łatwo stracić, korzystając ze zwykłych kart debetowych.

Nieuczciwi sprzedawcy

Podczas płacenia kartą debetową bądźmy czujni i nie spuszczajmy jej z oczu. Karta może zostać skopiowana przez nieuczciwego pracownika sklepu, a nasz kod PIN zapamiętany przez zmodyfikowany terminal lub podejrzany przez sprzedawcę.

Skimming, czyli przerobione bankomaty

Korzystając z bankomatu, uważnie mu się przyjrzyjmy, szczególnie dwóm elementom: podajnikowi, w który wkładamy kartę, oraz klawiaturze. Jeżeli elementy te nie są dokładnie spasowane z obudową lub w jakiś inny sposób wzbudzają podejrzenie, nie korzystajmy z tego bankomatu i najlepiej zgłośmy swoje podejrzenia firmie będącej właścicielem bankomatu. Dlaczego zwracać uwagę na te dwa elementy bankomatu? Ponieważ przestępcy w miejscu na kartę montują skaner, który ją kopiuje, a nakładka na klawiaturę zapamiętuje wpisywany numer PIN. Po kilku godzinach działania takiego zestawu przestępcy mogą skopiować nawet kilkaset kart i poznać ich PIN-y.
Przed skimmingiem możemy się uchronić, tylko zachowując czujność.

Uwaga na karty zbliżeniowe

Choć karty, którymi można płacić przez zbliżenie ich do terminalu, to stosunkowa nowość, istnieją sposoby na okradanie ich posiadaczy. Przestępcy mają sposoby na kopiowanie takich kart (nawet bezprzewodowo), ale kradzież pieniędzy jest możliwa nawet bez klonowania karty. Kiedy jeden przestępca płaci telefonem z **NFC***, włącza się aplikacja, która łączy się z identycznym telefonem wspólnika. Wspólnik w tym czasie przykłada telefon w pobliżu karty zbliżeniowej uprzednio upatrzonej ofiary i dane z karty są przesyłane do płacącego w sklepie. W ten sposób niczego nieświadomy przechodzień płaci za zakupy przestępców.
Jak się uchronić przed kradzieżą? Jeśli nie chcemy korzystać z płatności zbliżeniowych, poprośmy bank o zablokowanie tej funkcji, a jeśli jest to niemożliwe, nośmy kartę w etui (można je kupić za kilka złotych na aukcjach internetowych) nieprzepuszczającym fal elektromagnetycznych.

Fot.: Niebezpiecznik.pl

Fot.: krebsonsecurity.com

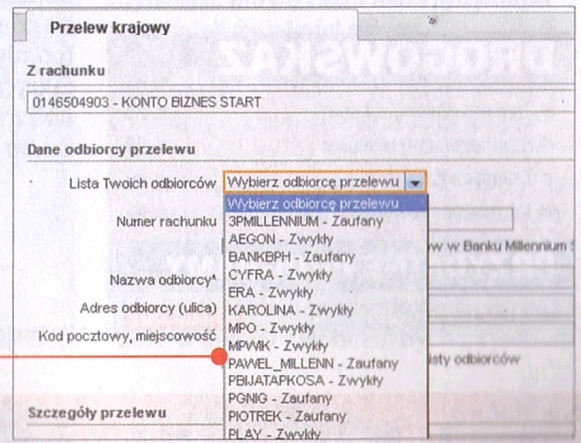
* Wyjaśnienie pojęcia w leksykonie na stronach 102–103

Zagrożenie czai się w skrzynce

O tym, że pomysłowość przestępców nie ma granic, przekonały się osoby, które mimo że opłaciły comiesięczne rachunki przez internet, otrzymują wezwanie do zapłaty. Do tego oszustwa nie jest potrzebna nawet specjalistyczna wiedza ani drogi sprzęt. Wystarczy zwykłe urządzenie wielofunkcyjne za kilkaset złotych ze skanerem i kolorową drukarką. Na czym więc polega cały proceder? Przestępcy włamują się do skrzynek pocztowych budynków mieszkalnych i kradną z nich rachunki, które zostawia listonosz. Następnie skanują rachunki, w programie graficznym podmieniają numery kont prawowitych odbiorców na własne i drukują rachunki. Następnie spreparowane rachunki trafiają do skrzynek pocztowych, z których je ukradziono. Niczego niepodejrzewający płatnik reguluje należność na poczcie, w sklepie czy z rachunku przez internet. Pieniądze trafiają na konto przestępcy, a nieświadomy klient otrzymuje wezwanie do zapłaty rachunku, za który należność uiścił na podmienione konto.

Jak się bronić

Jeżeli rachunki opłacamy przez internet, łatwo możemy uniknąć opisanego wyżej zagrożenia. Wystarczy podczas opłacania rachunków korzystać z listy zdefiniowanych odbiorów. Taką funkcję ma każde internetowe konto. Musimy jedynie poświęcić kilka minut na dodanie do listy numerów rachunków i danych adresowych odbiorców, którym często przelewamy pieniądze. Taki sposób ma dwie zalety – po pierwsze nie jesteśmy narażeni na oszustwo polegające na podmianie numeru konta na rachunku, a po drugie wygodniej i szybciej jest wykonać przelew, wybierając odbiorcę z listy, niż przepisywać za każdym razem numer konta i dane adresowe.



Więcej na: www.ebook4all.pl

6 Bezpieczne zakupy w sieci

Zakupów w sieci dokonuje prawie co drugi internauta. Dowiedzmy się, jak zadbać o bezpieczeństwo transakcji on-line

Zakupy w sieci, aukcje i wszelkie inne formy zawierania zdalnych umów o świadczenie usług to naturalna odpowiedź na nasze potrzeby. Wolny czas, który można poświęcić na tradycyjne zakupy, jest komfortem, na który nie zawsze możemy sobie pozwolić. **E-commerce*** przyciąga także niższymi cenami i szeroką ofertą dzięki łatwemu dostępowi do setek sklepów.

Niestety, zakupy on-line to nie to samo co obejrzenie produktu w sklepie, na którym wyraźnie podana jest cena. Zachłyśnięci wygodą internetowych zakupów zapominamy, że w sieci bardzo łatwo jest oszukiwać. A satysfakcja z zakupów to przede wszystkim poczucie zakupowego bezpieczeństwa on-line. Pod tym pojęciem kryje się całe spektrum zachowań, które powinny stać się dla nas nawykiem. Oszukani lub pozbawieni przysługujących nam praw możemy bowiem zostać na każdym etapie procesu zakupowego. Często przez własną nieuwagę i naiwność.

Poznajmy zasady bezpieczeństwa, zanim rozpoczniemy przygodę z branżą e-commerce. Począwszy od tak błahej sprawy jak komputer, za pomocą którego dokonujemy transakcji, poprzez wybór właściwego sklepu lub aukcji, dobór produktu (co nie zawsze jest łatwe), kontrolę nad faktycznymi wydatkami, a skończywszy na zapewnieniu możliwości zwrotu, gdy zakup nie spełni naszych oczekiwań. **kż**

DROGOWSKAZ

- Zanim zaczniemy zakupy s. 55
- Bezpieczeństwo zakupów s. 56
- Zakupy za granicą s. 59
- Jak pewnie i bezpiecznie płacić s. 61

PRZYDATNE PROGRAMY

- G Data IS 2014 **CD-KOD: 007**

* Wyjaśnienie pojęcia w leksykonie na stronach 102–103

Zanim zaczniemy zakupy

Z rozdziału 1 mogliśmy dowiedzieć się, jak zabezpieczyć komputer przed cyberprzestępcami. Zastosowanie się do opisanych tam reguł plus dbałość o aktualizację oprogramowania, a zwłaszcza przeglądarek internetowych, jest konieczne, zanim wejdziemy w świat zakupów on-line. Stosujmy również oprogramowanie chroniące transakcje bankowe. W przypadku pakietu G Data IS 2014 jest to moduł Bank Guard.

Wybór komputera

Zasiadając do komputera, z którego dokonamy transakcji, należy kierować się zasadą ograniczonego zaufania. Wykorzystujmy tylko nasz komputer, a nie przypadkowe urządzenie u znajomego lub, co gorsza, komputer w kafejce internetowej. Nigdy nie mamy gwarancji, że nieznany nam komputer będzie wolny od wirusów. Nawet tryb anonimowego przeglądania nie gwarantuje, że nie pozostawimy na dysku danych dotyczących naszej transakcji. Nie przechowujmy ważnych informacji, jak haseł w niezaszyfrowanej postaci, podobnie jak numerów kart, kodów CVV i dat ważności.

Źródło: Bezpieczeństwo i zaufanie, raport Ceneo Lato 2013

Jak wybrać zaufany sklep

Dobra reputacja powinna być wystarczającą rekomendacją dla sklepu, ale jak ją sprawdzić? Najpierw możemy przyjrzeć się opiniom w porównywarkach cen, na przykład ceneo.pl lub skapiec.pl, czy na serwisach z opiniami, jak opineo.pl. Gdy nie jesteśmy bywalcami e-sklepów, zaufajmy najbardziej znanym. Dobrym wskaźnikiem reputacji sklepów jest stosowanie

Czytelność witryny także może być jednym ze wskaźników jakości sklepu*

znaków jakości, na przykład TrustedShops. Czasem handlowcy umieszczają na stronach informacje o certyfikatach, których nie mają (na przykład ISO 9001:2000). Dlatego sam obrazek nie wystarczy, konieczny jest link do bazy zaufanych sklepów.

Cena to ważne kryterium przy wyborze sklepu, jednak superatrakcyjne oferty to także wabik na nieobeznanych z rynkiem

Eksperci G Data ostrzegają!
7000 różnych złośliwych programów po ia się w sieci każdego dnia.

Więcej na: www.ebook4all.pl

klientów. Często za niską ceną stoją dużo wyższe koszty dostawy niż w innych sklepach lub problemy z dostępnością towaru, który miał tylko przyciągnąć nas na daną witrynę.

Internet uwalnia nas od granic, ale starajmy się kupować w sklepach, do których łatwo będzie nam w razie problemów dotrzeć. Dobrą opcją jest odbiór osobisty.

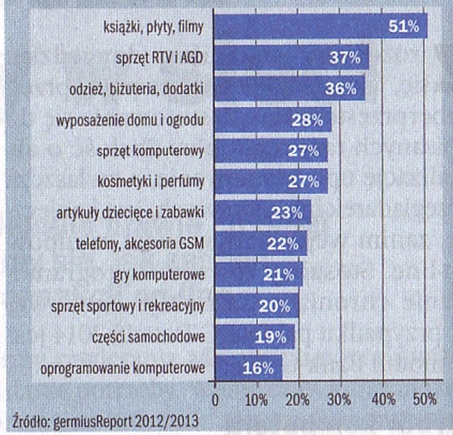
Gdy decydujemy się na zakup drogiego sprzętu albo opinie o sklepie nie są zadowalające, trzeba sięgnąć głębiej w sieć. Świetną pomocą są fora tematyczne, gdzie szybko uzyskamy odpowiedź na nurtujące nas pytania dotyczące renomy sklepu i znajdziemy doniesienia o naciągaczach grasujących na serwisach aukcyjnych. Celujmy w fora, gdzie liczba wątków i odpowiedzi jest duża, na przykład forum.nikoniarze.pl. Świadczy to o zaangażowaniu użytkowników. Komentujmy też nasze zakupy, to pomoże z kolei innym.

Aukcja czy sklep

Wiele osób staje przed dylematem – zakup na aukcji czy w sklepie? W praktyce wiele aukcji to oferty istniejących sklepów, dla których portale typu Allegro czy eBay to dodatkowy kanał dystrybucji. Gdy zdecydujemy się na zakup od osoby prywatnej, musimy uszanować ewentualne ograniczone prawo do gwarancji. W przypadku licencji upewnijmy się, czy produkt, na przykład pakiet oprogramowania, może być legalnie odsprzedawany.

Poza tym aukcja z ustaloną ceną Kup Teraz nie różni się od oferty sklepowej.

CO NAJCHĘTNIEJ KUPOWALIŚMY W INTERNECIE W 2012 ROKU



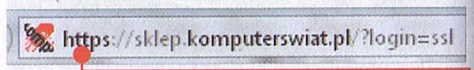
Źródło: germiusReport 2012/2013

Bezpieczeństwo zakupów

Kupiliśmy produkt, a on do nas nie dociera. Ktoś podszył się pod nasze konto i dokonał zakupów. Otrzymaliśmy wadliwy towar, ale nie mamy kontaktu ze sprzedawcą. Każda z takich sytuacji wiąże się ze szkodami finansowymi. Jak ich uniknąć?

Bezpieczne logowanie

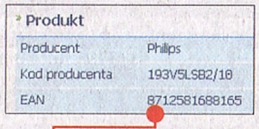
Sprawdźmy, czy witryna sklepu stosuje zabezpieczenia. Dotyczy to przede wszystkim strony logowania i stron, na których podawane są poufne dane. Zabezpieczenie



symbolizowane jest przez protokół https widoczny w pasku adresu przeglądarki przed adresem strony sklepu. Gdy brak zabezpieczeń SSL, sprawdźmy, czy nie można ich wymusić – formularz logowania zawiera na przykład pole bezpieczne logowanie.

Dane kontaktowe sklepu

Nie ufajmy sklepom, które podają skąpe dane kontaktowe, na przykład sam e-mail. Sklep powinien udostępniać takie informacje, jak adres, pod którym prowadzona jest działalność, informacje o firmie, dane umożliwiające inny niż elektroniczny kontakt, w tym numer telefoniczny (najlepiej również stacjonarny). Dobry kontakt przyda się podczas konsultacji w sprawie zakupu, ale również w przypadku reklamacji.

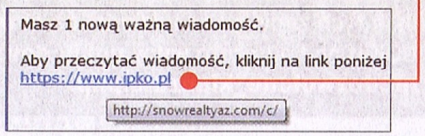


Kod produktu nadawany przez producenta (nie należy go mylić z kodem sklepowym) najlepiej identyfikuje produkt

Uważajmy na błędy, fałszywe odnośniki czy e-maile

Źródłem problemów mogą być literówki podczas wprowadzania adresu sklepu lub danych podczas zakupów. Błędnie wpisany adres może przekierować nas do podstawionej strony.

Pilnujmy odnośników, które prowadzą do sklepów. Te na stronach porównywarek i z opiniami są prawdziwe, ale na innych witrynach, a zwłaszcza **skrócone linki***, nie gwarantują bezpieczeństwa. Sprawdzajmy, czy linki w tekście nie prowadzą w inne niż spodziewane miejsce (wystarczy najechać kursorem myszy na odnośnik – wyświetli



KIEDY TRANSAKCJA LUB SKLEP SĄ PODEJRZANE

Powszechnie uznawana zasada brzmi: jeśli mamy wrażenie, że oferta wygląda zbyt pięknie, by była prawdziwa, to z pewnością tak jest. Pamiętajmy, że wybór sklepu jest równie istotny, jak wybór samego produktu. Gdy spełniony jest choćby jeden z poniższych warunków, powinniśmy zastanowić się, czy ktoś nie chce nas nabić w tak zwaną butelkę.

- Na stronie brak jakichkolwiek informacji kontaktowych, a także jednoznacznie identyfikujących sklep.
- Strona nie stosuje żadnych zabezpieczeń połączenia podczas dokonywania transakcji.
- Nie mamy innego wyboru płatności niż przelew.
- Brak opisu kupowanego produktu, a jedynie lakoniczna nazwa, która jednoznacznie nie identyfikuje tego, co kupujemy.
- Opis jest chaotyczny, pełen kolorowych dużych czcionek przeplatanych tekstem napisanym drobnym drukiem.
- Nie możemy znaleźć regulaminu, a zwłaszcza informacji dotyczących postępowania w przypadku zwrotu towaru, na przykład gdy stwierdzimy niezgodność z ofertą.
- Oferta wykorzystuje skrócony link, czyli nie wiadomo, czy nie prowadzi do fałszywej wersji witryny sklepu.
- Regulamin zawiera niedozwolone klauzule (patrz strona 58). Ich celem jest zazwyczaj utrudnienie klientowi egzekwowania należnych mu praw.

* Wyjaśnienie pojęcia w leksykonie na stronach 102–103

Więcej na: www.ebook4all.pl

NIEDOZWOLONE KLAUZULE W REGULAMINIE

Regulamin sprzedaży to bardzo ważny dokument, który precyzuje zasady, na jakich sklep prowadzi handel. Definiuje obowiązki oraz prawa konsumenta i sprzedawcy. Warto wiedzieć, że nie zawsze zapisy w regulaminie muszą być zgodne z prawem. W przypadku wątpliwości, a także innych problemów z wyegzekwowaniem warunków umowy zakupu, można zwracać się do Rzecznika Ochrony Praw Konsumentów lub UOKiK. Zapisy regulaminu, które są niezgodne z prawem i nie musimy się do nich stosować, określa się mianem niedozwolonych klauzul. Pełną listę tych zapisów znajdziemy na stronie UOKiK pod adresem **www.uokik.gov.pl/niedozwolone_klauzule.php**.

Sprzedawca nie ma między innymi prawa do:

- Narzucenia lokalizacji sądu, który będzie rozwiązywał ewentualne spory.
- Wskazywania firmy, do której należy odsyłać zwracany towar.
- Odliczenia kosztów wysyłki towaru od zwracanej kwoty w przypadku rozwiązania umowy.
- Nieponoszenia odpowiedzialności za błędy w opisie produktu na stronie z ofertą
- Uchylenia się od odpowiedzialności za uszkodzenie przesyłki i opóźnienia w dostawie.
- Żądania spisania protokołu uszkodzenia w obecności kuriera/dostawcy przesyłki.

się ramka z prawdziwym adresem). Upewnijmy się także co do poprawności wprowadzanych danych osobowych, zwłaszcza adresu e-mail.

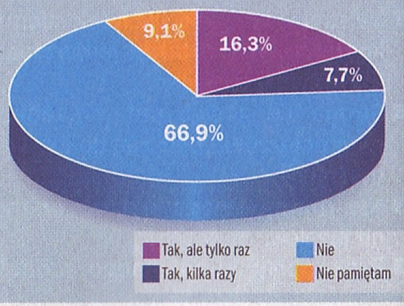
W przypadku zakupów on-line korespondencja poprzez e-mail jest czymś normalnym. Należy jednak pilnie kontrolować przysyłane listy. Fałszywy e-mail od cyberprzestępcy może wyglądać bardzo podobnie. Naszą uwagę powinny zwracać wszelkie nadmiarowe listy, a zwłaszcza te, w których proszeni jesteśmy o podanie dodatkowych informacji osobowych. Nigdy tego nie róbmy. Możemy skonsultować się z obsługą klienta telefonicznie i upewnić, czy dane działania są konieczne.

Po dokonaniu transakcji wskazane jest wykonanie kopii potwierdzenia zakupu. Zachowujmy wszelkie kwity otrzymane podczas wysyłania przesyłki lub odbioru od kuriera. Jeśli je wyrzucamy, to uprzednio zniszczone.

CENA CENIE NIERÓWNA

Sprzedawcy, śledząc naszą historię odwiedzin stron internetowych, mogą zaproponować cenę maksymalizującą szanse zakupu. Dlatego nie należy się dziwić, gdy ceny różnią się zależnie od tego, jak trafiliśmy na stronę danego sklepu.

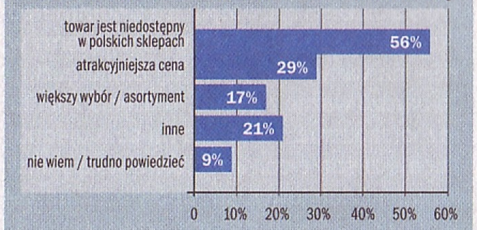
CZY ZOSTAŁEŚ KIEDYŚ OSZUKANY?



Zakupy za granicą

Zakupy w sklepach znajdujących się poza granicami Polski są coraz bardziej popularne – według raportu Gemius za 2012 rok tak kupuje już 15 procent internautów. Z aukcji za granicą korzysta natomiast 11 procent Polaków. Kupując za granicą, bardzo uważnie czytajmy regulaminy sklepów i zapoznawajmy się z zasadami sprzedaży.

DLACZEGO KUPUJEMY ZA GRANICĄ?



Źródło: germiusReport 2012/2013

Dodatkowe opłaty

Przy wyborze sklepu i oferty kierujmy się tymi samymi kryteriami, co przy selekcji w ramach naszego kraju. Szczególną uwagę zwracajmy na wszelkie dodatkowe informacje i opisy kosztów.

Ten niepozorny dopisek informuje nas, że Amazon jedynie pośredniczy w sprzedaży

Kupując na terenie UE, nie płacimy cła. Zakupy spoza Unii obciążone są opłatami zależnie od kraju pochodzenia. To, czy je poniesiemy, zależy od szczęścia i wartości przesyłki. Zakupione w USA towary warte do 45 euro mogą być zwolnione z opłat celnych i VAT-u. Towary o wartości do 150 euro mogą być zwolnione z cła, ale VAT będziemy musieli już zapłacić.

By poznać faktyczne opłaty w zagranicznym sklepie, złóżmy próbne zamówienie, a następnie je anulujmy przy podliczaniu kosztów. Tak dowiemy się również, czy sklep wysyła towary do Polski. Ryzyko oclenia maleje, gdy korzystamy ze zwykłej poczty, a nie kuriera, a przesyłka oznaczona jest jako Gift (podarunek) lub prywatna.

Możliwe problemy

Zakupy poza UE wiążą się z ryzykiem kłopotów z szybkim odzyskaniem pieniędzy, długotrwałą realizacją transakcji i dodatko-

PRZYDATNE INFORMACJE

- **www.trustpilot.com** – opinie o sprzedawcach z różnych krajów
- **isztar.mf.gov.pl:7080/taryfa_celna/web/main_PL** – informacje o kodach produktów i stawkach celnych
- **www.celina.krakow.uc.gov.pl/kalkulator/index.jsp** – kalkulator opłat celnych i VAT, wymaga danych z systemu ISZTAR (poprzedni link)
- **www.pricegrabber.com, www.nextag.com** – porównywarki cen dla rynku amerykańskiego
- **www.notanio.pl** – zbiór najważniejszych ofert z różnych porównywarek cen
- **www.cenowarka.pl/eu** – zestawienie ofert z różnych sklepów w całej Europie

Więcej na: www.ebook4all.pl

NOWA DYREKTYWA UE DOTYCZĄCA ZAKUPÓW ONLINE

Od 2014 roku na terenie całej Unii Europejskiej zacznie obowiązywać dyrektywa 2011/83/UE dotycząca e-commerce (kompletną treść dyrektywy znajdziemy w KŚ+ na wirtualnej płycie tej Biblioteczki). To bardzo ważne z punktu widzenia klienta rozporządzenie, które ma na celu ujednolicenie zasad e-commerce we wszystkich krajach członkowskich. Obowiązek udzielania dokładnych danych przedsiębiorcy oraz opisywania towaru sprawi, że kupując w sieci, będziemy czuli się bezpieczniej.

- Wprowadzony zostanie jeden 14-dniowy termin na odstąpienie od umowy zawartej on-line, o ile w umowie nie postanowiono inaczej, a o prawie do zwrotu towaru klient będzie musiał być powiadomiony. W przypadku braku tych informacji w umowie z klientem termin ten zostaje wydłużony nawet do 12 miesięcy po zakupie.
- Zwrot pieniędzy nastąpi w ciągu 14 dni od daty odstąpienia od umowy. Termin może być wydłużony do momentu otrzymania potwierdzenia zwrotu przez sprzedawcę.
- Czas dostawy nie może przekroczyć 30 dni. Można go skrócić na podstawie umowy pomiędzy sprzedawcą i kupującym. Niedotrzymanie tego terminu daje konsumentowi prawo do natychmiastowego rozwiązania umowy.
- Wystawiający na sprzedaż towar musi poinformować nabywcę o wszystkich kosztach, zobowiązaniach czasowych, jakie poniesie w związku z zakupem i komunikacją ze sklepem. Oferty produktowe muszą zawierać wszystkie elementy ceny, również te związane z kosztami dostawy i dodatkowych opłat w przypadku zakupów za granicą. Płatności dokonywane za pomocą kart kredytowych mogą być dodatkowo obciążane.
- Koszty konsultacji poprzez infolinię będą takie same jak w przypadku zwykłej rozmowy, a w przypadku produktów cyfrowych konieczne będzie dokładne wyspecyfikowanie kompatybilności ze sprzętem i oprogramowaniem.
- W trakcie zawierania umowy na odległość przez telefon sprzedawca ma obowiązek zidentyfikować się oraz określić cel przeprowadzanej rozmowy.
- Oferta internetowa musi zawierać również wszelkie informacje o możliwych ograniczeniach w związku z realizacją umowy. Konsument ma prawo otrzymać potwierdzenie zawartej transakcji na trwałym nośniku.
- Uzasadnienie przyczyn zwrotu towaru spoczywa na konsumencie, a zapewnienie udostępnienia wszelkich potrzebnych podczas zakupu informacji na przedsiębiorcy.

wymi zobowiązaniami. Pojęcie „free" nie zawsze oznacza „darmowy". Trzeba również pamiętać, że na serwisach aukcyjnych i w azjatyckich sklepach pojawia się dużo podróbek. Dlatego istotne jest dokładne studiowanie opisu i umiejętność czytania między słowami. Na poprzedniej stronie znajdziemy adresy stron z przydatnymi informacjami dla kupujących za granicą. By ułatwić zakupy on-line w ramach Unii Europejskiej, Komisja Europejska opracowała nową dyrektywę (patrz ramka ●). Będzie to dokument nadrzędny w stosunku do lokalnych przepisów.

Jak pewnie i bezpiecznie płacić

Teoretycznie najpewniejszą formą płatności jest opłata za pobraniem. Otrzymujemy towar do ręki prawie tak jak w sklepie. Prawie, bo zawsze pozostaje ryzyko otrzymania niewłaściwej lub uszkodzonej przesyłki. Na szczęście renomowany e-sklep nie będzie nam robił problemów ze zwrotem lub wymianą. Gdy wybierzemy opcję odbioru osobistego w placówce sklepu, sytuacja jest jeszcze bardziej komfortowa.

Karty kredytowe

Istotą e-commerce są jednak umowy na odległość i opłaty realizowane bezgotówkowo. Najlepiej w tym celu korzystać z kart kredytowych. W przeciwieństwie do zwykłych przelewów czy przekazów pieniężnych, dają one większe szanse (współpraca banku) na odzyskanie gotówki w przypadku problemów. Dla zakupów on-line wystarczy **wirtualna karta kredytowa*** przedpłacona. Działa tak samo jak tradycyjna, a jest bezpieczniejsza dzięki temu, że jej limit nie przekracza aktualnie wpłaconych na jej konto środków. Zwykle to kwota równa planowanym wydatkom on-line.

Systemy zabezpieczające sklepów

Sklepy i serwisy aukcyjne często oferują również własne systemy zabezpieczające przepływ pieniędzy od kupującego do sprzedawcy. W Allegro.pl jest to Program Ochrony Kupujących (**poznaj.allegro.pl/pok**). Gdy nie otrzymamy towaru, możemy liczyć na 100-procentowy zwrot poniesionych kosztów do 10 000 złotych. Sklepy korzystające z certyfikatu Trusted Shops ● mają do dyspozycji podobny system ochrony kupującego.

Uniwersalne systemy płatności

Największe bezpieczeństwo i wygodę płatności on-line zapewnią uniwersalne systemy płatności. Zamiast podawać za każdym razem dane konta, wystarczy zarejestrować je raz w jednym z systemów. W Polsce najpopularniejszy jest PayU (**www.payu.pl**). Inne systemy to PayPal (**www.paypal.com**) czy Skrill (**www.skrill.com**). Dodatkowa korzyść to gwarancja ochrony transakcji – w przypadku PayPal spór ze sprzedawcą można otworzyć nawet 45 dni po wniesieniu opłaty za towar, a PayU działa podobnie jak Program Ochrony Kupujących Allegro.

BEZPIECZNE ZAKUPY MOBILNIE

Samo zabezpieczenie smartfona odpowiednim oprogramowaniem (patrz rozdział 10) nie wystarczy. Trzeba pamiętać jeszcze o kilku zasadach.

- Nie korzystajmy z niezabezpieczonych hotspotów.
- Nie instalujmy oprogramowania o nieznanej reputacji, spoza sklepów z aplikacjami. Wyjątek to aplikacje dedykowane – dla portali aukcyjnych lub banków.
- Unikajmy przechowywania poufnych danych w pamięci smartfona, a jeśli już to robimy, to w zaszyfrowanej postaci.
- Hasło i login do naszego konta bankowego podajemy tylko w aplikacji bankowej. Inne programy nie mają prawa uzyskać do nich dostępu.

* Wyjaśnienie pojęcia w leksykonie na stronach 102–103

Więcej na: www.ebook4all.pl

7 Prywatność, anonimowość

Użytkownicy internetu mają różne obawy związane z ochroną swojej prywatności. Z tego rozdziału dowiemy się, jak o nią dbać zarówno w sieci, jak i we własnym komputerze

Stare internetowe przysłowie mówi: prywatność i anonimowość w internecie nie istnieje. To, co raz wrzucimy do sieci, trudno jest usunąć – informacje są archiwizowane i błyskawicznie powielane. Mówi się też, że internet nie zapomina i nie wybacza. Były członek kabaretu OT.TO stracił posadę kierownika Domu Kultury, gdy wyszło na jaw, że umieścił w internecie prześmiewczą piosenkę na temat władz dzielnicy, w której pracował. Jedną z kelnerek popularnej amerykańskiej restauracji wyrzucono z pracy po tym, jak upublicznione przez nią zdjęcie rachunku jednego z klientów restauracji stało się internetowym viralem – zdaniem firmy ich pracownica dokonała poważnego naruszenia prywatności klienta. W tym rozdziale uczymy się na błędach innych – poznamy sprytne sposoby anonimowego korzystania z sieci i sprawdzimy, co internet o nas wie. Zobaczymy też, jak wygląda procedura usuwania swojego konta z serwisów społecznościowych. Ponieważ często zapominamy, że to my sami ujawniamy większość informacji na swój temat, a bywa i tak, że rozdajemy osobiste informacje na lewo i prawo – na zdjęciach, w wypowiedziach na stronach i serwisach społecznościowych – nauczymy się rozważnego dzielenia się informacjami w świecie internetu. **mm**

DROGOWSKAZ

- Optymalne ustawienia prywatności w serwisach społecznościowych s. 63
- Zamykamy swoje konta w serwisach społecznościowych s. 67
- Co internet o mnie wie s. 69
- Surfujemy bez śladów w komputerze s. 71
- Usuwamy ślady przeglądania z komputera s. 72
- Trzy sposoby na anonimowy dostęp do internetu s. 72

PRZYDATNE PROGRAMY

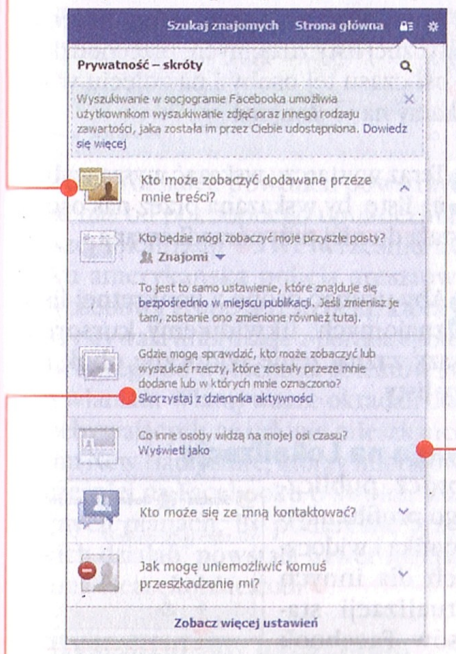
- CCleaner 4.04 CD-KOD: 003
- PirateBrowser 0.6b CD-KOD: 019
- Tor Browser Bundle 2.3 CD-KOD: 027

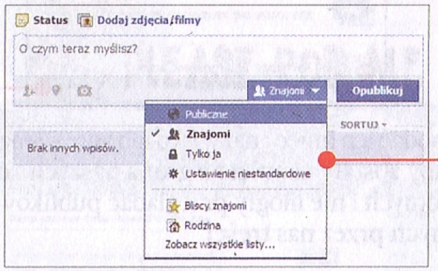
Optymalne ustawienia prywatności w serwisach społecznościowych

Domyślne ustawienia prywatności w popularnych serwisach społecznościowych nie gwarantują ochrony prywatnych informacji. Zobaczmy, jak je zmienić.

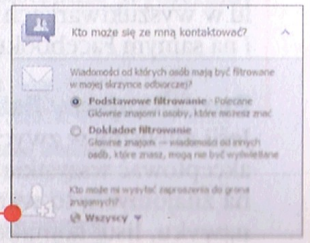
Facebook

1 Dostęp do ustawień naszej prywatności uzyskamy, klikając na ikonę. W pierwszej sekcji ustalamy, kto może zobaczyć nasze posty, czyli aktualizacje statusów wyświetlane na naszej tablicy. Statusy są domyślnie publicznie dostępne – dla naszego bezpieczeństwa powinny być widoczne tylko dla naszych znajomych. Ustawienia prywatności poszczególnych postów można też kontrolować bezpośrednio w miejscu ich publikacji. Możemy tu też sprawdzić, jak wygląda nasza tablica z perspektywy osób odwiedzających nasz profil. Wart uwagi jest również tak zwany dziennik aktywności, w którym zobaczymy historię naszej aktywności na FB, i zdjęcia, na których nas oznaczono.



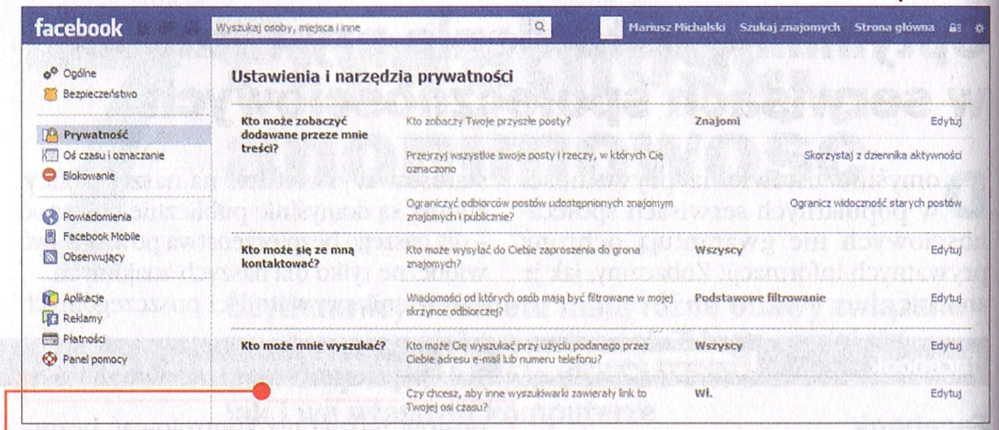


2 W drugiej sekcji możemy określić, kto może się z nami kontaktować i wysyłać zaproszenia do grona znajomych.

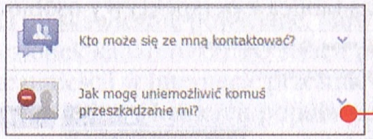


Eksperci G Data ostrzegają!
Nowe zagrożenia na Androida pojawia się średnio co 22 sekundy.

Więcej na: www.ebook4all.pl



3 Trzecia sekcja pozwala łatwo zablokować irytujące nas osoby – wystarczy



podać ich imię i nazwisko lub adres e-mail, aby zostały usunięte z grona naszych znajomych i nie mogły przeglądać publikowanych przez nas treści.

4 Dostęp do większej liczby ustawień uzyskamy, klikając na przycisk Zobacz więcej ustawień. Znajdziemy tu wartą uwagi sekcję, pozwalającą wyłączyć możliwość znalezienia naszego profilu w wyszukiwarkach internetowych, jak i na samym Facebooku.

Porządkujemy listę znajomych

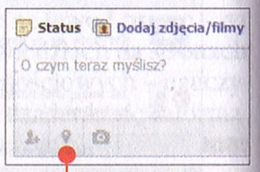
Jeśli mieliśmy w zwyczaju automatycznie akceptować wszystkie zaproszenia do grona znajomych, to warto pozbyć się tego nawyku, listę kontaktów uporządkować i zadbać o to, by do znajomych nie przyjmować ludzi, których tak naprawdę nie znamy – z perspektywy bezpieczeństwa nie ma żadnego racjonalnego powodu, by udostępniać im informacje o swoim życiu osobistym.

1 Aby dodać wybraną osobę do tematycznej listy znajomych, przechodzimy do osi czasu tej osoby i na zdjęciu w tle klikamy na Znajomi.

2 Teraz wystarczy wskazać myszą wybraną listę, by wskazana przez nas osoba została do niej przyporządkowana.

3 Aby usunąć osobę z konkretnej listy znajomych, likwidujemy kursorem myszy zaznaczenie widoczne obok nazwy listy.

Uwaga na Lokalizację



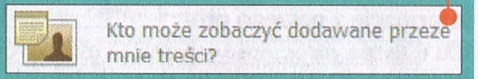
Oprócz publicznego profilu użytkownika i widocznych dla innych aktualizacji statusów Facebook oferuje funkcję o nazwie Lokalizacja (podobnie jak Twitter i Foursquare), która pokazuje światu, gdzie teraz jesteśmy.

USUWAMY ZNACZNIK ZE ZDJĘCIA LUB WYDARZENIA

Użytkownicy Facebooka mogą oznaczać nas na zdjęciach i w postach. Zobaczmy, jak usunąć niechciany znacznik.

1 Aby usunąć znacznik z danego zdjęcia lub wydarzenia, klikamy na ikonę i z rozwijanego menu wybieramy opcję Zgłoś/usuń znacznik.

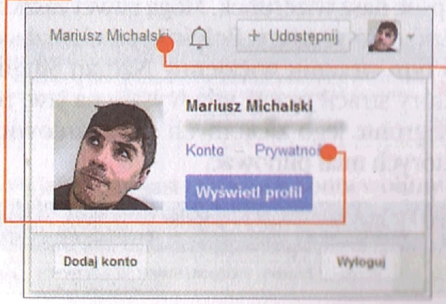
2 Możemy także usunąć znaczniki z wielu zdjęć jednocześnie. W tym celu klikamy na, wybieramy opcję i Skorzystaj z dziennika aktywności.



3 Naciskamy przycisk Zdjęcia i wybieramy te z nich, z których chcemy usunąć znaczniki. Zmiany zatwierdzamy kliknięciem na opcję Zgłoś / usuń znaczniki.

Zdrowy rozsądek powinien powstrzymywać nas od pochopnego upubliczniania naszej lokalizacji. We wrześniu 2010 roku amerykańska policja aresztowała trzyosobową grupę przestępczą, która wykorzystywała informacje z portalu społecznościowego do wybierania obiektów swoich włamań. Włamywacze okradali domy przebywających na urlopie mieszkańców stanu New Hampshire, którzy informowali wcześniej na Facebooku o swoich wakacyjnych planach. By podkreślić ryzyko takich działań, powstała nawet specjalna strona PleaseRobMe.com.

2 Klikamy na swoje imię i nazwisko lub adres e-mail w prawym górnym rogu ekranu, a następnie wybieramy opcję.

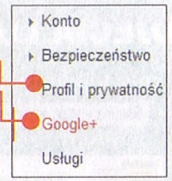


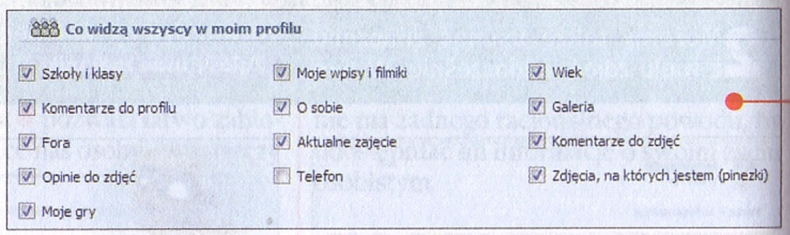
Optymalizujemy ustawienia prywatności w Google+

1 Otwieramy stronę Google+ i logujemy się na swoje konto.

Więcej na: www.ebook4all.pl

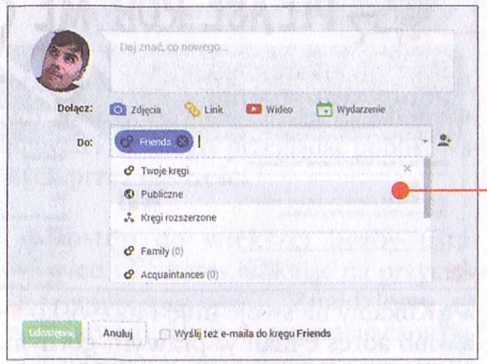
3 Ustawienia prywatności znajdziemy w dwóch sekcjach: ● i ●. W sekcji Profil i prywatność możemy zdecydować, które informacje z naszego profilu (Ustaw widoczność w profilu) mają być widoczne dla poszczególnych osób, kontaktów z kręgów lub być publiczne. Warto zwrócić też uwagę na sekcję Widoczność w sieci – ustalamy tutaj, które kontakty będą widoczne w naszym profilu. Niewłaściwe osoby w gronie znajomych mogą negatywnie wpływać na naszą reputację w sieci i psuć nasz wizerunek. Mogą nawet zaszkodzić nam w pracy. Boleśnie przekonał się o tym strażnik więzienny Nathan Singh, który stracił pracę, gdy wyszło na jaw, że w gronie jego znajomych są więźniowie, których miał pilnować.





4 Ważnym ustawieniem jest sekcja Zdjęcia – możemy tu określić, czy w naszym profilu będzie widoczna karta Zdjęcia i czy inni użytkownicy mogą nas oznaczać na przesyłanych zdjęciach – tagi będą połączone z naszym profilem Google.

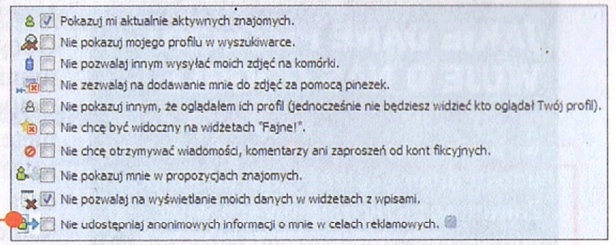
5 Gdy dajemy znać na Google+, co u nas nowego, zwracajmy uwagę, czy post udostępniamy właściwym osobom. Każdy post ma specjalne pole z podsumowaniem tego, komu zostanie udostępniony ●. Publikując informacje bardzo osobiste, należy zwrócić szczególną uwagę na ustawienia ich prywatności – nie musimy, a nawet nie powinniśmy informować o wszystkim swojego szefa.



Dostrajamy opcje prywatności w NK

1 W chodzimy na nk, klikamy na ● i wybieramy opcję ●.

2 W sekcji ● decydujemy, które informacje o nas będą dostępne dla wszystkich. Ponieważ dane te będą widoczne publicznie, powinniśmy chronić prywatne zdjęcia i inne osobiste dane.

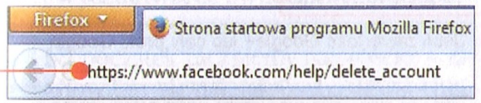


3 W dziale ● możemy ograniczyć możliwość wyszukania naszego profilu, zabronić oznaczania nas na zdjęciach, wyłączyć opcję pokazującą innym, że oglądaliśmy ich profil, a także zrezygnować z udostępniania informacji o nas w celach reklamowych.

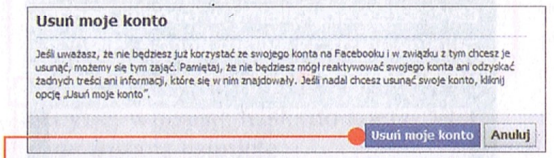
Zamykamy swoje konta w serwisach społecznościowych

Usuwamy konto z Facebooka

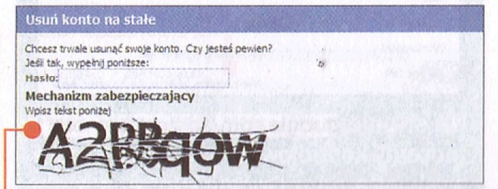
Facebook udostępnia dwa sposoby zamknięcia konta. Pierwszy to trwałe usunięcie konta, bez możliwości przywrócenia go w przyszłości. Druga metoda to tak zwana dezaktywacja konta, która spowoduje, że nasza oś czasu zniknie od razu z Facebooka, inni użytkownicy nie będą mogli nas wyszukać ani przeglądać naszych danych. Dezaktywowane konto można w każdej chwili przywrócić, logując się w serwisie za pomocą e-maila i hasła – oś czas zostanie w pełni przywrócona wraz z listami znajomych i zdjęciami.

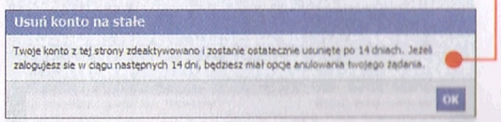


1 Aby trwale usunąć konto z Facebooka, wchodzimy na stronę ●, klikamy na przycisk ●, wypełniamy dane w mechanizmie zabezpieczającym ● i naciskamy OK.



2 Facebook poinformuje nas o rozpoczęciu dwutygodniowej procedury usuwania danych ●.



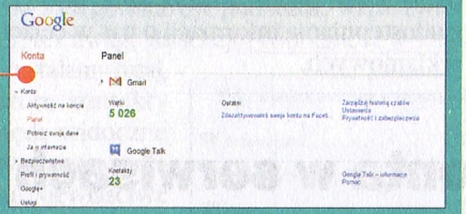


3 Jeżeli zamiast usuwania konta wolimy je dezaktywować, klikamy na przycisk ●, Bezpieczeństwo, Dezaktywuj konto i naciskamy Potwierdź.

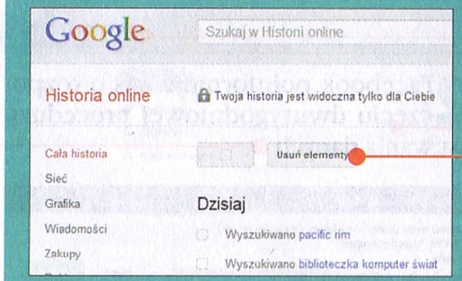
Więcej na: www.ebook4all.pl

JAKIE DANE PRZECHOWUJE O NAS GOOGLE

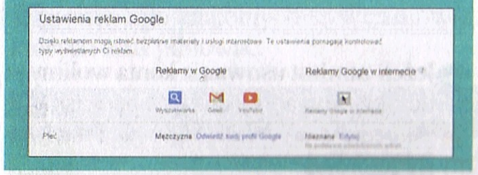
Każdy użytkownik Google ma swoją wirtualną kartotekę, która zawiera udostępnione przez nas informacje. Zawartość teczki możemy sprawdzić pod adresem www.google.com/dashboard/.



Na stronie dostępnej pod adresem www.google.com/history/ możemy zobaczyć, czego szukaliśmy w Google, będąc zalogowanym na swoim koncie. Historię można usunąć.



Na stronie google.com/ads/preferences/ możemy kontrolować typy reklam, które wyświetla nam Google. Na tej stronie zobaczymy też, jak Google nas postrzega na podstawie naszych poprzednich wyszukiwań i odwiedzanych witryn.

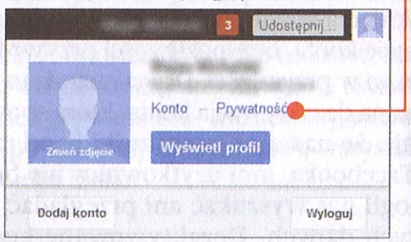


Usuwamy swój profil z Google+

Google+, podobnie jak Facebook, po zamknięciu konta nie usuwa naszych danych w 100 procentach. Nasze kręgi zostaną usunięte, ale osoby w nich obecne pozostaną na naszej liście kontaktów w Gmailu. Procedura zamykania konta usunie nasze wpisy, komentarze i +1-ki. Nie zostaną usunięte utworzone przez nas społeczności, strony ani żadne zdjęcia (będą nadal dostępne w Picasie). Nasze opinie zamieszczone w usłudze Google+ Lokalnie wciąż będą widoczne w Mapach Google.

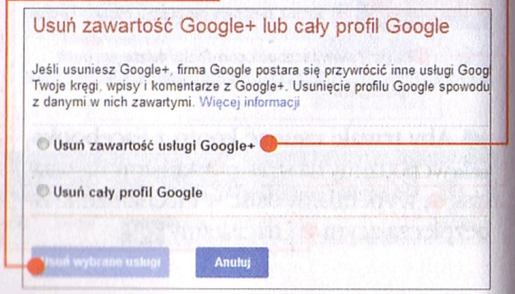
1 Logujemy się na swoje konto w Google+.

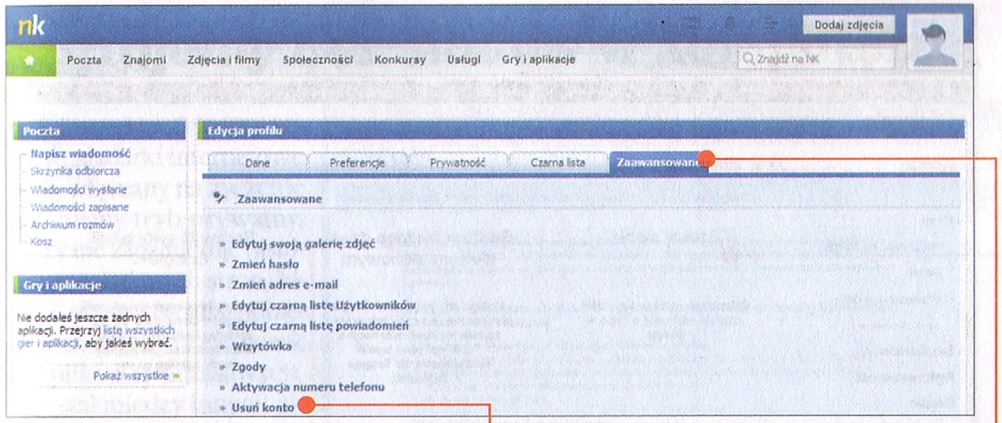
2 Klikamy na swoje imię i nazwisko lub adres e-mail w prawym górnym rogu ekranu i wybieramy opcję.



3 Przechodzimy do sekcji Konto, Zarządzanie kontem i klikamy na Usuń profil i powiązane funkcje Google+.

4 Wybieramy kolejno, Wymagane: i klikamy na.





Usuwamy konto na NK

Usunięcie konta na NK jest nieodwracalne i spowoduje skasowanie naszej galerii zdjęć, listy znajomych, a także wypisanie z klas i szkół. Nie jest jednak równoznaczne z usunięciem naszych danych osobowych z bazy serwisu – o to będziemy musieli poprosić NK za pomocą formularza kontaktowego.

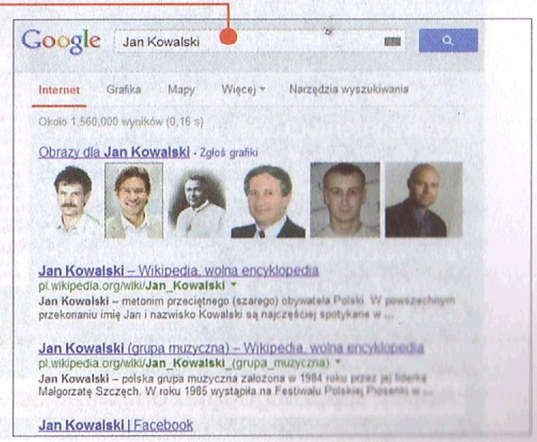
1 Klikamy na opcję profil widoczną w prawym górnym rogu i wybieramy Edycja profilu.

2 Przechodzimy do zakładki, wybieramy opcję i potwierdzamy swoją decyzję, wpisując hasło do konta. Nasze dane zostaną usunięte.

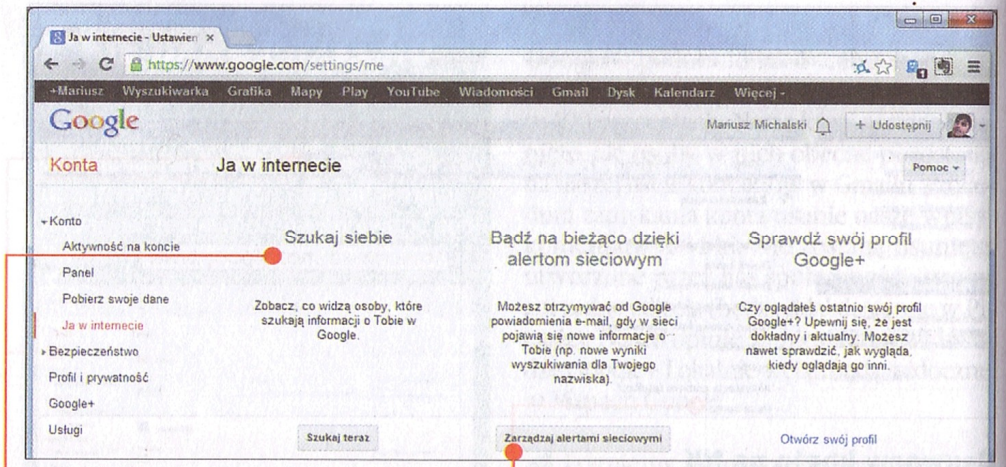
Co internet o mnie wie

Oprócz nas samych informacji na nasz temat mogą szukać w internecie nowo poznane osoby, znajomi znajomych, rekruterzy i pracodawcy. Zobaczmy zatem, jak sprawdzić, co jest o nas w najpopularniejszej wyszukiwarce świata, czyli Google.

1 Na początek zaczniemy najprościej – zachowamy się tak, jak osoba, która chce znaleźć o nas informacje – wpisujemy w Google swoje imię i nazwisko. Analogicznie warto sprawdzić wyniki wyszukiwania dla naszego adresu e-mail, numeru telefonu i pseudonimu, którym posługujemy się w sieci.



Więcej na: www.ebook4all.pl

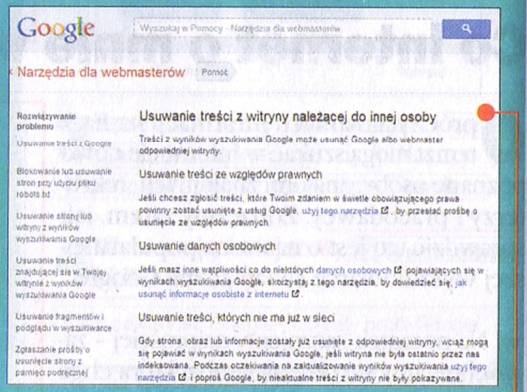


2 Google przygotowało specjalny mechanizm, który pozwala sprawdzić, co widzą inne osoby, gdy szukają nas w wyszukiwarce Google – strona jest dostępna pod adresem www.google.com/settings/me.

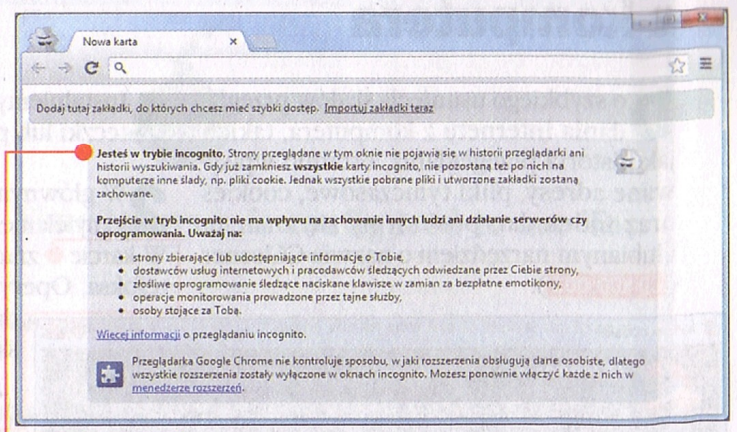
3 Do dyspozycji mamy też funkcję ustawiania alertów, dzięki którym możemy otrzymywać powiadomienia o tym, że nasze dane osobowe (imię i nazwisko, adres e-mail) zostały opublikowane w sieci.

JAK USUNĄĆ INFORMACJE O SOBIE Z WYNIKÓW WYSZUKIWANIA GOOGLE

Google wyświetla w wynikach wyszukiwania tylko te informacje, które są publicznie dostępne w sieci. Ponieważ wyszukiwarka nie może usuwać zawartości stron internetowych, wymazanie konkretnych wyników wyszukiwania z Google nie spowoduje usunięcia tej treści z internetu. Jeśli chcemy usunąć konkretne informacje o sobie z sieci, powinniśmy zacząć od skontaktowania się z webmasterem strony, na której zostały one opublikowane, i poprosić o stosowne zmiany. Po usunięciu danych Google zarejestruje zmiany i niechciane informacje przestaną pojawiać się w wynikach wyszukiwania. Więcej informacji o usuwaniu treści z Google znajdziemy na stronie https://support.google.com/webmasters/answer/1663688?hl=pl.

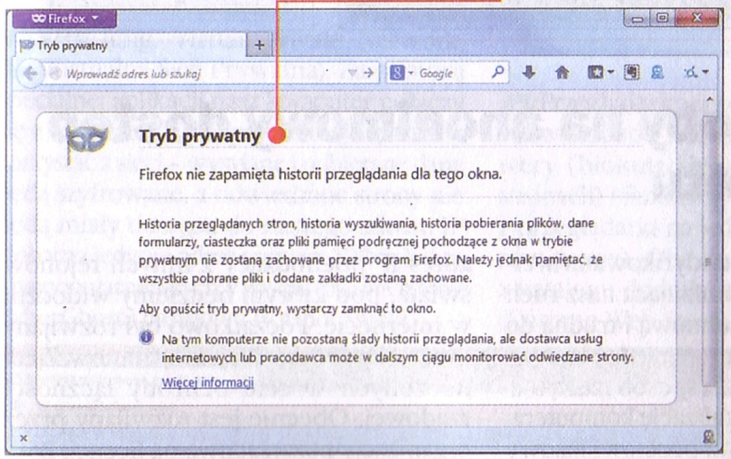


Surfujemy bez śladów w komputerze



Wszystkie czołowe przeglądarki internetowe mają włączany na życzenie tak zwany tryb prywatny, który nie zapamiętuje historii przeglądanych stron, historii wyszukiwania, pobieranych plików, ciasteczek ani plików tymczasowych. Powstał między innymi po to, abyśmy mogli dyskretnie przeglądać strony internetowe bez konieczności późniejszego usuwania śladów z komputera ręcznie – wystarczy zamknąć okno trybu prywatnego, aby nie zachowały się o nim żadne informacje. Tryb prywatny nie zapewnia anonimowości w internecie.

1 W Chrome funkcja ta nosi nazwę Tryb incognito, który włączamy za pomocą przycisku ☰ i opcji Nowe okno incognito. Możemy też użyć kombinacji klawiszy ctrl+shift+N. W Firefoksie jest to tak zwany Tryb Prywatny – włączamy go przez menu Firefox, Nowe okno prywatne lub za pomocą kombinacji klawiszy ctrl+shift+P. W przeglądarce Internet Explorer tryb prywatny funkcjonuje pod nazwą Przeglądanie InPrivate. Włączyć go można za pomocą kombinacji klawiszy ctrl+shift+P lub przez opcję ⚙, Bezpieczeństwo i Przeglądanie InPrivate. Opera nazywa go Karta prywatna (lub Okno prywatne), a w makowym Safari jest to po prostu Przeglądanie prywatne.



2 Gdy zamkniemy wszystkie karty incognito, nie pozostaną po nich w komputerze żadne ślady. Aby opuścić tryb prywatny, wystarczy zamknąć jego okno.

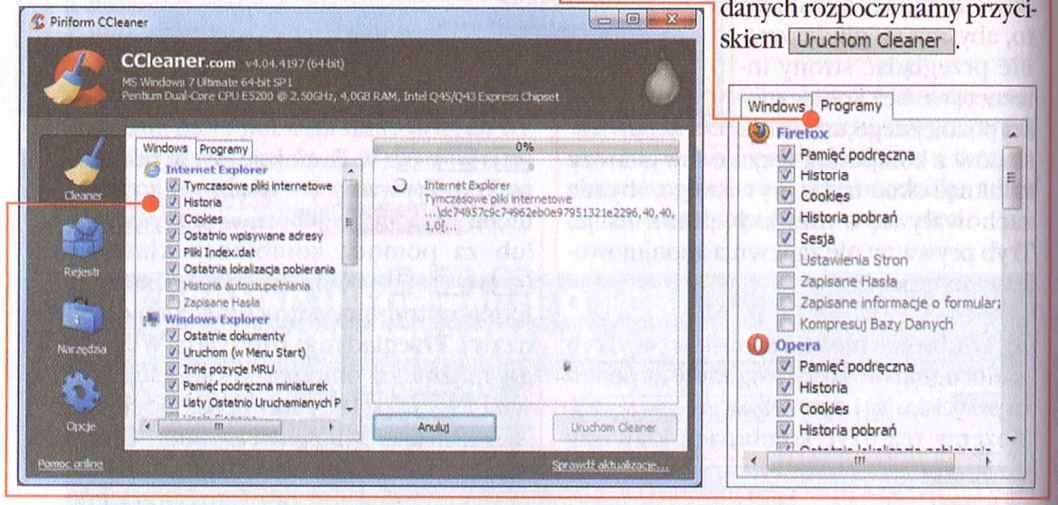
Więcej na: www.ebook4all.pl

Usuwamy ślady przeglądania z komputera

Do szybkiego usunięcia śladów przeglądania internetu z komputera, takich jak historia przeglądania, ostatnio wpisywane adresy, pliki tymczasowe, cookies oraz index.dat, posłużymy się znanym i lubianym narzędziem o nazwie CCleaner (CD-KOD: 003).

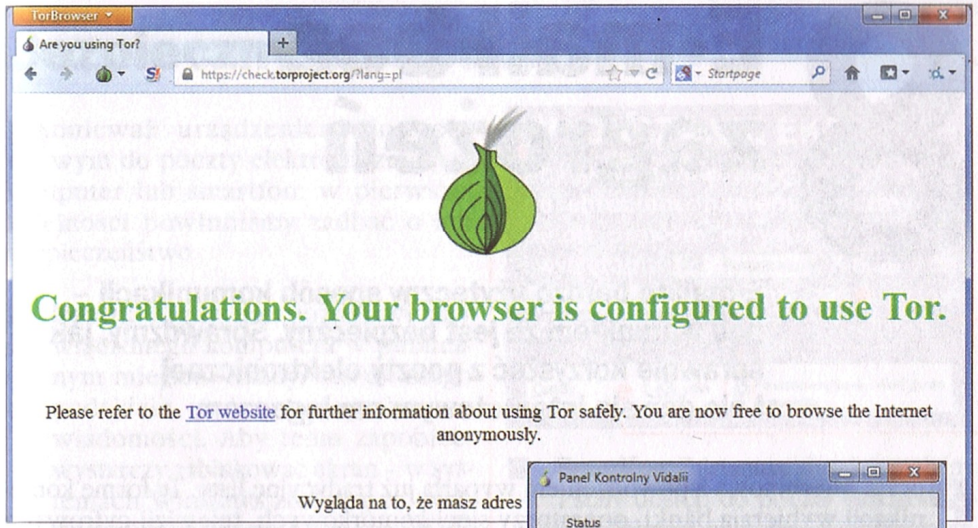
1 Instalujemy CCleanera z płyty Biblioteczki lub przez aplikację KŚ+.

2 W głównym oknie programu wskazujemy elementy historii do usunięcia. W karcie znajdziemy opcje dotyczące Firefoksa, Opery i Chrome. Wymazywanie danych rozpoczynamy przyciskiem Uruchom Cleaner.



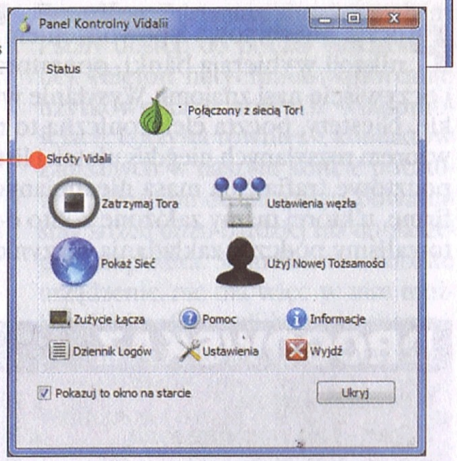
Trzy sposoby na anonimowy dostęp do internetu

1 **Tor** CD-KOD: 027 (zmodyfikowana wersja Firefoksa anonimizująca nasz ruch sieciowy) tworzy anonimową i trudną do wyśledzenia sieć połączeń między komputerami, ukrywając w ten sposób naszą tożsamość i faktyczną lokalizację komputera. Tor przypisuje naszemu pecetowi losowy adres IP pochodzący z innych rejonów świata, pod którym będziemy widoczni w internecie. Początkowo był rozwijany przez Marynarkę Wojenną Stanów Zjednoczonych w celu ochrony łączności rządowej. Obecnie jest rozwijany przez organizację pozarządową na licencji BSD.



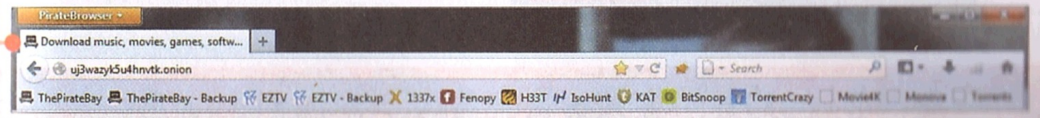
Tor działa niestety wolniej niż typowe przeglądarki – coś za coś. Jest darmowy i po polsku.

Specjalną wersję Tora wydał niedawno z okazji swoich 10 urodzin serwis The Pirate Bay. Przeglądarka z Zatoki Piratów nazywa się PirateBrowser CD-KOD: 019 i powstała w celu omijania cenzury w internecie. Program bazuje na angielskiej wersji Firefoksa 23 Portable.



2 **VPN** (ang. Virtual Private Network, Wirtualna Sieć Prywatna). Za pomocą specjalnej aplikacji nasz komputer połączy się z serwerem VPN, przez który będziemy korzystać z sieci – wysyłane i odbierane dane będą szyfrowane, a odwiedzane strony nie będą miały dostępu do naszego adresu IP (zobaczą jedynie adres serwera VPN). Jeden z najpopularniejszych VPN-ów to komercyjny CyberGhost i darmowy Hotspot Shield.

3 Przeglądarka internetowa uzbrojona w dodatki anonimizujące typu Ghostery (blokuje śledzące nas skrypty na stronach) i FoxProxy (przekierowuje ruch z przeglądarki na jeden lub więcej serwerów proxy). Oba dodatki można pobrać z katalogu dodatków Firefoksa i Chrome (Chrome Web Store).



Więcej na: www.ebook4all.pl

8 E-mail bez zagrożeń

E-mail to bardzo użyteczny sposób komunikacji – pod warunkiem że jest bezpieczny. Sprawdźmy, jak sprawnie korzystać z poczty elektronicznej i nie dać się internetowym naciągaczom

Poczta internetowa z powodzeniem wyparła już tradycyjne listy. Tę formę komunikacji wybierają banki, operatorzy sieci komórkowych, telewizji cyfrowych i oczywiście nasi znajomi. Wysyłanie wiadomości e-mail jest proste, darmowe i szybkie. Niestety, poczta elektroniczna to również doskonałe narzędzie marketingowe, wzorem rozsyłanych niegdyś ulotek i listów z łańcuszkami szczęścia na nasze skrzynki pocztowe trafia cała masa niechcianych wiadomości. Niektóre wysyłane są przez firmę, u której mamy założone konto e-mail, zgodnie z regulaminem, który zaakceptowaliśmy podczas zakładania skrzynki. Pozostałe wiadomości to tak zwany spam. Oprócz typowo reklamowego przesłania niechciane wiadomości mogą stanowić dla nas duże niebezpieczeństwo – na przykład zawierają wirusy, konie trojańskie lub podszywając się pod ważne dla nas instytucje (na przykład bank), próbują wyłudzić poufne informacje. Pocztą elektroniczną powinniśmy się więc posługiwać rozsądnie, według określonych reguł. Ponieważ nie wszystko jednak da się przewidzieć, warto skorzystać z mechanizmów chroniących nas przed niebezpieczeństwami związanymi z używaniem poczty e-mail. **aś**

DROGOWSKAZ

- Bezpieczny komputer s. 75
- Spam – walka z niechcianą pocztą s. 76
- Solidne konto pocztowe z dobrym filtrem s. 77
- Ochrona poczty e-mail w G Data s. 78
- Szyfrowanie wiadomości e-mail s. 80
- Phishing, czyli wyłudzanie danych s. 80

PRZYDATNE PROGRAMY

- G Data InternetSecurity 2014 CD-KOD: 007
- Poczta systemu Windows CD-KOD: 020
- Thunderbird 17.0.8 CD-KOD: 026

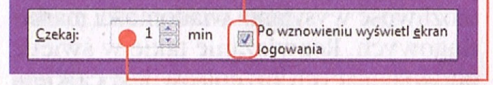
Bezpieczny komputer

Ponieważ urządzeniem dostępowym do poczty elektronicznej jest komputer lub smartfon, w pierwszej kolejności powinniśmy zadbać o ich bezpieczeństwo.

- **Pecet:** Nigdy nie pozostawiajmy włączonego komputera w publicznym miejscu. Każdy, kto do niego podejdzie, może przeczytać nasze wiadomości. Aby temu zapobiec, wystarczy zablokować ekran – w systemach Windows zrobimy to, wciskając jednocześnie klawisze (nasze konto musi być chronione hasłem). Zapominalscy powinni skorzystać z systemowej funkcji wygaszania ekranu z opcją ochrony hasłem. Więcej na temat zagrożeń dla komputera przeczytamy w rozdziale 1.
- **Konto pocztowe:** Zakładając konto pocztowe, wybierzmy sprawdzonego i solidnego usługodawcę (na przykład serwis gmail.com). Pamiętajmy również, aby konto zabezpieczyć trudnym do zgadnięcia hasłem – więcej na temat tworzenia bezpiecznych haseł przeczytamy w rozdziale 9. Jeżeli korzystamy z webmaila, na stronie WWW nie używajmy funkcji zapamiętywania haseł przez przeglądarkę, szczególnie pracując na nie swoim komputerze. Ich odzyskanie jest bardzo proste i można to zrobić kilkoma kliknięciami.

WYGASZANIE EKRANU

Aby skonfigurować wygaszanie ekranu chronione hasłem, klikamy na pulpit prawym przyciskiem myszy i wybieramy Personalizuj. Klikamy na Wygaszacz ekranu, ustawiamy czas i zaznaczamy opcję.



- **Smartfon:** Zaletą smartfona jest mobilny i stały dostęp do poczty elektronicznej. Telefon natychmiast informuje użytkownika o nowych wiadomościach, korzysta również z kontaktów zapisanych w naszym koncie pocztowym. Dostępu do smartfona powinniśmy strzec dużo bardziej niż do naszego komputera. Smartfon to osobiste urządzenie, nie ma więc w nim możliwości konfiguracji kont użytkowników. Każdy, kto dostanie go w swoje ręce, może sprawdzić lub wysłać wiadomości e-mail. Podobnie jak komputer, także smartfon możemy zabezpieczyć, na przykład kodem PIN lub wzorem graficznym. O tym, jak skutecznie zabezpieczyć smartfon, przeczytamy w rozdziale 10.
- **Program antywirusowy:** Koniecznie zainstalujemy w komputerze dobry program antywirusowy, oprócz ochrony plików będzie on również sprawdzał nasze e-maile i blokował spam.

G DATA Eksperci G Data radzą
Niezwłocznie kasuj wszelki spam i zawsze unikaj
erania zawartych w nim linków czy załączników.
G DATA

Więcej na: www.ebook4all.pl

Spam – walka z niechcianą pocztą

Spam to rozsyłane masowo do wielu odbiorców wiadomości e-mail o identycznej treści. W praktyce najczęściej jest to jednak niezamawiana przez nas oferta handlowa. Mimo że e-maile takie są zakazane przez polskie i unijne prawo, to wiele firm oferujących darmowe konta pocztowe w regulaminie zastrzega sobie możliwość wysyłania wiadomości marketingowych. Rozwiązanie takie w świetle obowiązujących przepisów jest całkiem legalne, ponieważ podczas rejestracji wyrażamy zgodę na otrzymywanie spamu. Spam to jednak nie tylko oferty handlowe, mogą to być również e-maile o charakterze niekomercyjnym, społecznym lub politycznym. Możliwość rozsyłania darmowych reklam to sposób na dotarcie do odbiorcy dla wielu firm – szczególnie naciągaczy. Ze względu na społeczną niechęć i brak akceptacji dla spamu szanujące się firmy nie korzystają z tego typu reklamy.

Czy spam jest szkodliwy

Zjawisko spamu niesie ze sobą wiele niebezpieczeństw: powoduje niepotrzebne obciążenie łączy internetowych i serwerów pocztowych, rozprzestrzenia wirusy i trojany oraz niezbezpieczne dla odbiorcy wiadomości, naraża firmy na dodatkowe koszta związane z koniecznością ochrony przed spamem i narusza prywatność odbiorców.

Jak walczyć ze spamem

Najważniejszą rolę w walce z niechcianymi wiadomościami e-mail mają administratorzy serwerów pocztowych. Po pierwsze każdy serwer poczty wychodzącej musi wymagać autoryzacji (podczas wysyłania wiadomości musimy podać dane naszego konta), w walce ze spamem pomocne są również filtry antyspamowe i tak zwana szara lista (Graylisting). Serwer wyposażony w taki mechanizm tymczasowo odrzuca wiadomości od nierozpoznanych nadawców. Jeżeli wiadomość nie jest spamem, zostanie ponowiona próba wysłania i zakończy się sukcesem.

Ochrona przed spamem dotyczy także nas! Nigdy nie odpowiadajmy na takie wiadomości (warto oznaczyć wiadomość jako spam w programie pocztowym). Pamiętajmy również, aby nie publikować naszego adresu e-mail w internecie – podając go na forach lub portalach społecznościowych, spróbujmy go zmodyfikować, tak aby osoba chcąca do nas napisać, domyśliła się, że musi go zmienić: na przykład znak @ możemy zastąpić **(a)** lub **(at)**, ewentualnie zastąpić . wyrazem **(kropka)**.

arkadiusz.swiostek(a)komputerswiat.pl
arkadiusz.swiostek(at)komputerswiat.pl
arkadiusz.swiostek@komputerswiat(kropka)pl

Dzięki temu roboty spamerskie przeszukujące strony internetowe pod kątem adresów nie będą w stanie odszyfrować naszego prawidłowego adresu.

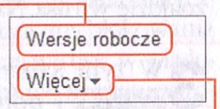
Oprócz wyuczonych nawyków i stosowania się do tych zasad warto korzystać z aplikacji pomagających nam ustrzec się przed spamem, a w szczególności filtrów antyspamowych. Zobaczmy, jakie mechanizmy możemy samodzielnie zastosować, by cieszyć się pocztą pozbawioną niepotrzebnych wiadomości.

Solidne konto pocztowe z dobrym filtrem

Godną polecenia usługą jest konto pocztowe Gmail. Wbudowane w nie funkcje antyspamowe działają sprawnie i zwykle dużo lepiej niż u innych darmowych usługodawców. Co więcej, wcale nie musimy rezygnować z dotychczasowych kont. Możemy bowiem wykorzystać Gmail do filtrowania naszej poczty. Zobaczmy, jak to zrobić.

1 Otwieramy stronę **www.gmail.com** i logujemy się do naszego konta pocztowego. Jeżeli go jeszcze nie mamy, klikamy na UTWÓRZ KONTO i wypełniamy formularz.

2 Po zalogowaniu się do konta Gmail podświetlamy wskaźnikiem myszy ostatnią pozycję (na przykład ●) i klikamy na ● i na Spam, aby sprawdzić wiadomości, które filtr zakwalifikował jako spam.



3 Jakość działania filtru zależy również od nas. Warto więc zgłaszać administratorom spam, który przedostał się do skrzynki odbiorczej. W tym celu zaznaczamy taki e-mail ● i klikamy na ❗.

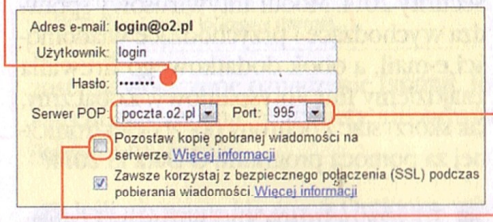
Dodajemy inne konto

Usługa Gmail pozwala również dodać inne konta, tak aby serwer spawdzał je automatycznie i pobierał z nich wszystkie nowe wiadomości. Zaletą takiego rozwiązania jest wykorzystanie sprawnie działającego filtru antyspamowego z Gmaila oraz prostsza obsługa – sprawdzamy tylko jedną skrzynkę.

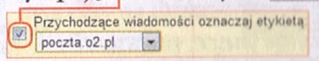
1 Aby dodać zewnętrzne konto pocztowe, będąc zalogowanym w serwisie Gmail, klikamy na ⚙ i na Ustawienia.

2 Klikamy na Konta i wybieramy opcję Dodaj posiadane konto pocztowe POP3. W nowo wyświetlonym oknie wpisujemy adres e-mail, z którego chcemy pobierać pocztę, i klikamy na Dalej.

3 W następnym oknie wpisujemy hasło ● i odznaczamy opcję ● (nie ma potrzeby przechowywać starych wiadomości na serwerze). Adres serwera POP3 i port ● oraz zabezpieczenie SSL powinny zostać automatycznie właściwie wykryte. W razie problemów musimy te parametry zweryfikować z danymi podawanymi przez firmę obsługującą nasze konto pocztowe.



4 Warto jeszcze nadać etykietę (e-maile łatwiej wtedy odnaleźć) każdej wiadomości przysłanej z tego konta. W tym celu zaznaczamy opcję ●. Klikamy na Dodaj konto ».



5 Jeżeli chcemy, aby nadal to konto było naszym głównym adresem mailowym, musimy zaznaczyć jeszcze opcję Tak, chcę wysyłać wiadomości jako login@o2.pl, w następnym oknie klikamy na Dalej, pozostawiając domyślne ustawienia.

Więcej na: www.ebook4all.pl

6 Musimy także zdecydować, z którego konta będzie domyślnie wysyłana poczta. Traktując serwis Gmail tylko jako filtr antyspamowy, zaznaczamy Wyślij przez o2.pl serwery SMTP, wpisujemy hasło i weryfikujemy parametry serwera SMTP naszego głównego konta.

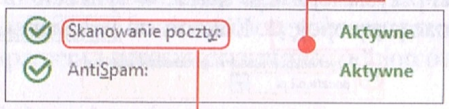
7 Sprawdzamy swoje stare konto pocztowe i odszukujemy wiadomość e-mail od nadawcy Zespół produktu Gmail i klikamy na umieszczony w niej link.

8 Na koniec powracamy do klienta Gmail i klikamy na ⚙, Ustawienia i na Konta. Jeżeli chcemy, aby dodane, zewnętrzne konto było naszym głównym, klikamy obok niego na ustaw jako domyślny. Ustawienie to spowoduje, że wszystkie e-maile będą wysyłane właśnie z tego konta.

Ochrona poczty e-mail w G Data

Osoby używające programów pocztowych (na przykład Microsoft Outlook, Thunderbird, Poczta systemu Windows) mają do dyspozycji jeszcze jeden stopień ochrony przed spamem. Dobry program antywirusowy z funkcjami internetowymi. Taką właśnie aplikacją jest G Data Internet-Security 2014. Moduł antywirusowy sprawdza wychodzące i przychodzące wiadomości e-mail, a obok dodatkowego firewalla znajdziemy filtr antyspamowy. Zobaczmy, jak skorzystać z ochrony poczty elektronicznej za pomocą programu G Data IS 2014.

1 To, czy ochrona antywirusowa i antyspamowa jest aktywna, możemy sprawdzić w głównym oknie programu ●.



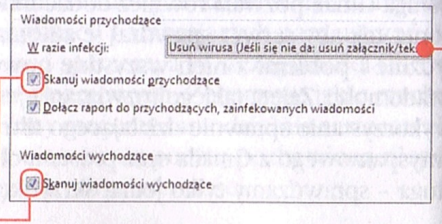
2 Na początku sprawdzimy ustawienia skanera poczty. Klikamy na ● i wybieramy ⚙ Zaawansowane... Sprawdzamy, czy zaznaczone są opcje skanowania poczty przychodzącej ● oraz wychodzącej ● oraz konfigurujemy akcję, jaką program ma wykonać, jeżeli w dostarczonej wiadomości znajdzie wirusa. Najrozsądniej wybrać ●.

3 W tym samym oknie klikamy na Więcej... i porównujemy ustawione w nowo wyświetlonym oknie porty serwerów POP, IMAP, SMTP z ustawionymi w naszym programie pocztowym.

Filtr antyspamowy

Moduł, który chroni programy pocztowe przed spamem w programie G Data, jest bardzo rozbudowany. Zobaczmy, na które funkcje zwrócić uwagę.

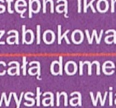
1 W głównym oknie programu klikamy na AntiSpam:, a następnie wybieramy ⚙ Zaawansowane..., aby przejść do ustawień filtra.



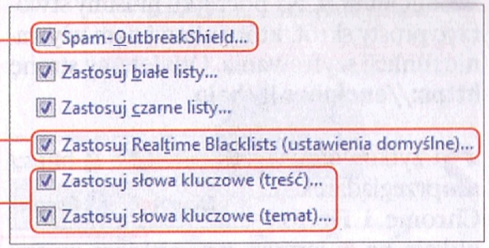
THUNDERBIRD I POCZTA SYSTEMU WINDOWS

Thunderbird CD-KOD: 026 to znany i ceniony program pocztowy, który domyślnie ma włączony filtr antyspamowy. Warto wiedzieć jednak, jak pomóc mu tropić adresy spamerów. Jeżeli do skrzynki odbiorczej przedostanie się niechciana poczta, klikamy na nią, a następnie poniżej, w oknie podglądu, klikamy na przycisk Niechciana. W ten sposób dodamy etykietę do poczty, którą uznaliśmy za spam. Aby ją usunąć, klikamy na ☰, Narzędzia i na Usuń niechciane wiadomości z folderu.

Poczta usługi Windows Live jest bezpłatnym, intuicyjnym i funkcjonalnym programem pocztowym, z którego mogą skorzystać wszyscy użytkownicy WIndows (CD-KOD: 020). W głównym oknie mamy dostępną ikonę ●, która pozwala zablokować ● nadawcę lub całą domenę, z której została wysłana wiadomość spam.

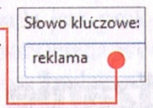


2 G Datę wyposażono w dwa automatycznie działające mechanizmy blokowania spamu. Funkcja ● zwalcza wirusy w wiadomościach, jeszcze zanim ich sygnatury zostaną opracowane. Natomiast ● pobiera listy spamerów z trzech serwerów i na ich podstawie blokuje niechciane wiadomości.



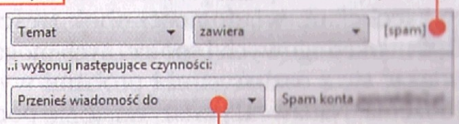
3 Elementami uzupełniającymi filtry antyspamowe w klientach pocztowych są funkcje ●. Działają one bardzo podobnie – pierwsza filtruje treść, druga – temat wiadomości. Aby dodać własne słowa kluczowe, klikamy na Zastosuj słowa kluczowe (treść)...

4 Następnie klikamy na Nowy..., podajemy słowa ●, które znajdujemy w niechcianych wiadomościach, i klikamy na OK.



5 Wszystkie wiadomości, które G Data zidentyfikuje jako spam, zostaną oznaczone. Jeżeli wiadomość jest podejrzana, w temacie zobaczymy **[Podejrzenie o spam]**, jeśli jest spamem, do tematu wiadomości zostanie dołączone oznaczenie **[spam]**. Jeżeli chcemy zmienić te etykiety, klikamy na Reakcja... i na Zmień...

6 Jeśli używamy Microsoft Outlooka, wiadomości zostaną przeniesione do folderu AntiSpam. W przypadku innych klientów musimy ręcznie stworzyć regułę. Na przykład, aby utworzyć ją w Thunderbirdzie, klikamy na ☰, dwa razy na funkcję Filtrowanie wiadomości i na Nowy... Tworzymy regułę sprawdzającą temat i wpisujemy ●. Następnie definiujemy akcję ●. Klikamy na OK.



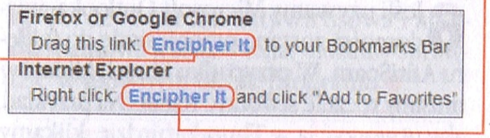
Więcej na: www.ebook4all.pl

Szyfrowanie wiadomości e-mail

Komunikacja za pomocą wiadomości e-mail jest na ogół bezpieczna, są jednak sytuacje, w których potrzebujemy możliwie najwyższego poziomu bezpieczeństwa. Aby zabezpieczyć się przed odczytaniem wiadomości przez niepowołane osoby, możemy jej treść zaszyfrować za pomocą hasła. Hasło zaś podajemy adresatowi za pomocą innego kanału – na przykład wysyłając mu SMS lub przekazując podczas rozmowy telefonicznej. Sprawdźmy, jak szyfrować e-maile.

1 Do szyfrowania wykorzystamy serwis **encipher.it**. Na początku musimy stworzyć prosty skrót, który ułatwi nam używanie funkcji szyfrowania. Otwieramy stronę **https://encipher.it/help**.

2 Użytkownicy przeglądarek Chrome i Firefox klikają na lewym przyciskiem myszy i trzymając go, przenoszą link na pasek zakładek. Użytkownicy Internet Explorera klikają na prawym przyciskiem myszy i wybierają Dodaj do ulubionych...



3 Przechodzimy do klienta pocztowego otworzonego w przeglądarce – na przykład Gmail, i klikamy na UTWÓRZ.

4 Wpisujemy nadawcę, temat oraz treść, a następnie klikamy na Encipher It.

5 W nowo wyświetlonym oknie wpisujemy hasło i klikamy na .

6 W następnym oknie klikamy na No. Treść naszej wiadomości zostanie zmieniona na ciąg znaków. Taki e-mail możemy wysłać naszemu adresatowi, podając mu hasło, którego użyliśmy do szyfrowania.

7 Odbiorca po otrzymaniu wiadomości musi ją odszyfrować. Jeżeli ma dodany na pasku zakładek skrót, wystarczy, że kliknie na niego i poda hasło.

8 Z mechanizmu szyfrującego i deszyfrującego możemy również skorzystać bezpośrednio ze strony **https://encipher.it**. Aby zaszyfrować tekst, wklejamy go do pola tekstowego i klikamy na .

Phishing, czyli wyłudzanie danych

Niechciane wiadomości obok treści marketingowych i społecznych mogą wiązać się z oszustwami i próbami wyłudzenia. Nadawca, podszywając się pod ważne i wzbudzające zaufanie instytucje (banki, urzędy), stara się wyłudzić od nas poufne dane. Tego typu działanie nazywane jest phishingiem. Poznajmy schematy działania cyberprzestępców i dowiedzmy się, jak obronić się przed phishingiem.

Jakie dane są wyłudzane

Phishing to jedno z największych niebezpieczeństw czyhających na internautę, ponieważ łupem hakerów padają dane, które bezpośrednio wiążą się ze stratami finansowymi. Na celowniku cyberprzestępców wyłudzających dane za pomocą phishingu są najczęściej banki, instytucje finansowe typu PayPal i serwisy aukcyjne. Tam następuje obrót realnym pieniądzem, stawka jest więc bardzo wysoka. Na czarnym rynku wyceniane są więc nasze konta pocztowe i w serwisach społecznościowych. Dostęp do informacji zbieranych przez Facebook wyceniany jest na około 6 dolarów. Jeszcze więcej warte są dane do zalogowania się do konta Gmail. Nic dziwnego, takie konto to skarbnica informacji o nas – jeżeli użytkownik konta korzysta z telefonu z Androidem, Google wie, gdzie się porusza, gdzie mieszka, jakie witryny odwiedza, ma dostęp do jego książki teleadresowej i karty kredytowej powiązanej ze sklepem Google Play.

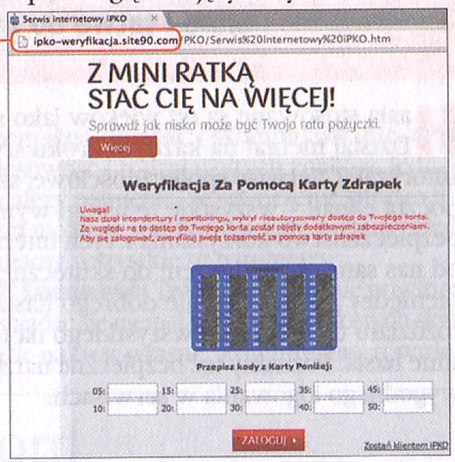
Jak działa phishing

Schemat działania cyberprzestępców jest prosty i zwykle się powiela. Na naszą skrzynkę pocztową wysyłane są wiadomości e-mail z prośbą o zalogowanie się do systemu bankowego czy konta pocztowego. Wygląd takiego e-maila jest praktycznie identyczny jak korespondencja wysyłana przez instytucję, za którą podaje się nadawca. W jej treści najczęściej znajduje się link przenoszący nas do strony logowania. Również ta strona najczęściej do złudzenia przypomina witrynę instytucji – różnią ją tylko detale i to na nie musimy zwracać uwagę.

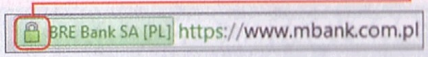
Jak uchronić się przed phishingiem

Każdy może stać się ofiarą phishingu, dlatego zawsze dokładnie sprawdzajmy wiadomości przed podjęciem jakichkolwiek kroków:

- **Sprawdźmy nadawcę** wiadomości, powinna być wysłana z domeny instytucji, od której dostaliśmy wiadomość.
- Wiadomość powinna być **kierowana do nas,** treść nie może być zbyt ogólna. Wiadomość powinna być także poprawna pod względem językowym.



- Jeżeli w mailu otrzymamy **link do systemu logowania**, dokładnie go sprawdźmy. W adresie musi być poprawna domena banku (przykład phishingu na użytkowników banku PKO z próbą wyłudzenia danych – niewłaściwa domena), a połączenie musi być szyfrowane .



- Nie reagujmy na **komunikaty o zagrożeniach** nakłaniające do natychmiastowego podania poufnych danych. Nigdy nie przesyłajmy w e-mailu hasła ani numeru karty kredytowej. Instytucje **nigdy** o nie nie proszą, zwłaszcza za pomocą wiadomości e-mail.

Więcej na: www.ebook4all.pl

9 Bezpieczne hasła

Korzystając z internetu, nie unikniemy stosowania haseł. Warto poznać zasady ich tworzenia, aby były silne i łatwe do zapamiętania

Hasła stosowane są od wieków jako skuteczny sposób na uwierzytelnienie osób. Dzisiaj niemal na każdym kroku stykamy się z tą najprostszą i najtańszą formą autoryzacji. Serwisy społecznościowe, sklepy internetowe, bankowość elektroniczna, poczta e-mail – wszystkie te usługi wymagają od nas rejestracji i logowania. Dlatego bezpieczeństwo korzystania z tych internetowych serwisów w dużym stopniu zależy od nas samych, a kluczem do skutecznej ochrony naszych danych, prywatności czy pieniędzy jest stworzenie dobrego hasła i odpowiednie jego zabezpieczenie. Z tego rozdziału dowiemy się wszystkiego na temat haseł – jakich unikać oraz jak tworzyć silne hasła. Poznamy też bezpieczne narzędzia do przechowywania naszych haseł oraz wygodnego logowania w serwisach. **tpa**

DROGOWSKAZ

- Co to są bezpieczne hasła s. 83
- Tworzymy bezpieczne hasła s. 86
- Menedżery haseł s. 87

PRZYDATNE PROGRAMY

- KeePass CD-KOD: 010
- KeePass spolszczenie CD-KOD: 011
- LastPass CD-KOD: 014

Co to są bezpieczne hasła

Zadaniem każdego systemu zabezpieczeń na hasło jest skuteczne ograniczenie dostępu do naszych danych niepowołanym osobom. Po stronie użytkownika takiego systemu pozostaje stworzenie bezpiecznego hasła, czyli takiego, które jest nie tylko mocne (trudne do złamania lub odgadnięcia dla innych), ale również łatwe do zapamiętania dla nas. O bezpieczeństwie naszego hasła decyduje również stosowanie kilku podstawowych reguł. Dowiedzmy się zatem, co to jest silne hasło oraz jakich haseł nie powinniśmy używać.

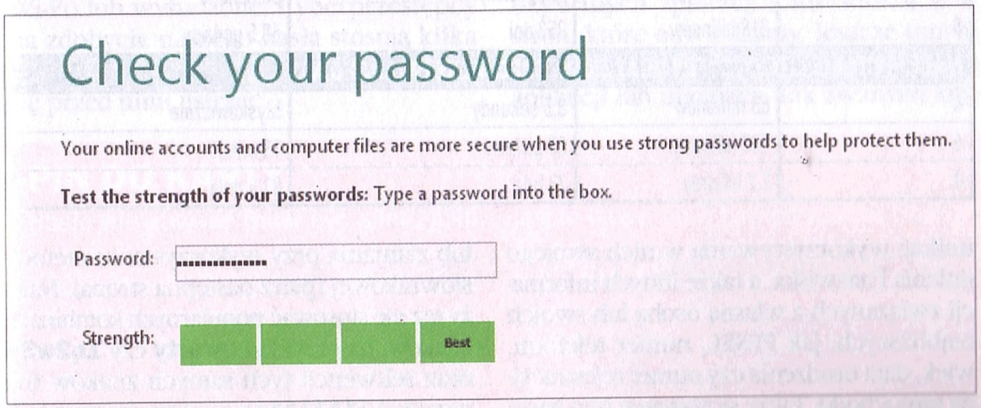
JEDNO DO WSZYSTKICH

Wiele osób korzysta z jednego hasła do logowania się w wielu serwisach i usługach. Jest to bardzo wygodne, ale z pewnością nie stanowi zbyt dobrego zabezpieczenia. Jeśli nasze hasło zostanie wykradzione z jednego serwisu, możemy stracić kontrolę nad wszystkimi swoimi kontami. Takie same hasło możemy zastosować jedynie do mało istotnych dla nas serwisów.

Jakie hasło to hasło mocne

Mocne (silne) hasło to hasło, którego ewentualne złamanie trwa bardzo długo i jest trudne do odgadnięcia nawet przez naszych bliskich. O sile hasła decyduje zatem jego długość i skomplikowanie, czyli losowość i rodzaj użytych znaków. Jednak należy pamiętać, że stworzenie silnego hasła możliwe jest tylko wtedy, gdy uwzględniamy wszystkie te parametry.

- **Losowość:** Tworzone hasła nie powinny składać się niemal wyłącznie z prostych słów jak nazwy własne. Powinniśmy również



Siłę hasła możemy sprawdzić, korzystając z wielu serwisów internetowych. Uwaga! Należy używać tylko zaufanych stron, na przykład www.microsoft.com/security/pc-security/password-checker.aspx

Eksperci G Data radzą
Do każdego konta używaj innego hasła składają o się z cyfr, znaków oraz małych i dużych liter.

Więcej na: www.ebook4all.pl

LICZBA KOMBINACJI A SKOMPLIKOWANIE HASŁA

DŁUGOŚĆ HASŁA	LICZBA MOŻLIWYCH KOMBINACJI	CZAS POTRZEBNY DO ZŁAMANIA HASŁA	
		ZWYKŁY PECET	SUPERKOMPUTERY
TYLKO CYFRY (10 ZNAKÓW)			
4	10 000	błyskawicznie	błyskawicznie
6	1 milion	błyskawicznie	błyskawicznie
8	100 milionów	10 sekund	błyskawicznie
TYLKO MAŁE LITERY LUB TYLKO WIELKIE LITERY (26 ZNAKÓW)			
4	456 976	błyskawicznie	błyskawicznie
6	308,9 miliona	30 sekund	błyskawicznie
8	200 miliardów	348 minut	3,5 minuty
MAŁE I WIELKIE LITERY (52 ZNAKI)			
4	7,3 miliona	błyskawicznie	błyskawicznie
6	19 miliardów	33 minuty	19 sekund
8	53 biliony	6 dni	15 godzin
MAŁE I WIELKIE LITERY ORAZ CYFRY (62 ZNAKI)			
4	15 milionów	2 sekundy	błyskawicznie
6	57 miliardów	1,5 godziny	56 sekund
8	218 bilionów	253 dni	60,5 godziny
MAŁE I WIELKIE LITERY, CYFRY ORAZ ZNAKI SPECJALNE (96 ZNAKÓW)			
4	85 milionów	8,5 sekundy	błyskawicznie
6	782 miliardy	22 godziny	13 minut
8	7,2 biliarda	23 lata	83,5 dnia

unikać wykorzystywania w nich swojego imienia i nazwiska, a także innych informacji związanych z własną osobą lub swoich najbliższych, jak PESEL, numer telefonu, wiek, data urodzenia czy numer rejestracyjny samochodu. Także stosowanie jako hasło własnych identyfikatorów (nazw użytkowników) nie jest dobrym pomysłem, nawet jeśli zmienimy w nim wielkość liter czy też napiszemy je wspak. Hasła typu **tomek80** czy też **barcelona** są bardzo łatwe do ogadnięcia lub złamania przy wykorzystaniu metody słownikowej (patrz następna strona). Należy też nie stosować popularnych kombinacji znaków, na przykład **qwerty** czy **1q2w3e** oraz sekwencji tych samych znaków (na przykład **11111111**), ponieważ nawet jeśli takie hasło jest bardzo długie – jest słabe.

■ **Rodzaj użytych znaków:** Hasło powinno składać się ze znaków z jak największego zbioru. Powinniśmy więc unikać tworzenia haseł zawierających wyłącznie cyfry czy też małe litery. Najlepiej, gdy zawiera cyfry, małe i wielkie litery oraz znaki specjalne.

■ **Długość hasła:** Im hasło dłuższe, tym silniejsze. Jednak bardzo długie hasło jest trudne do zapamiętania. Poza tym hasło powinniśmy wpisywać szybko. Przy dużej liczbie znaków wprowadzanie go na klawiaturze (szczególnie na smartfonach) może być utrudnione i łatwo o pomyłkę. Dlatego ośmioznakowe hasło o wysokim stopniu skomplikowania powinno zapewnić wysoki poziom bezpieczeństwa. Dla ważnych usług warto zastosować nawet 14-znakowe hasło.

Jak łamane jest nasze hasło?

Żadne hasło nie daje nam stuprocentowej pewności zabezpieczenia, ponieważ nawet najdłuższe i najbardziej skomplikowane hasło może zostać podpatrzone, kiedy je wpisujemy, podsłuchane (na przykład przy korzystaniu z niezabezpieczonej sieci Wi-Fi) lub wyłudzone. Cyberprzestępcy na zdobycie naszego hasła stosują kilka metod – poznajmy je, aby wiedzieć, jak się przed nimi ustrzec.

■ **ŁAMANIE HASŁA**

Najczęstszymi metodami do złamania hasła przez cyberprzestępców jest metoda słownikowa i brute-force (brutalnej siły). Pierwsza z nich opiera się na bazie najczęściej używanych lub prawdopodobnych słów. Są one kolejno wybierane i używane do próby zalogowania. Dlatego proste słowa nie są najlepszym pomysłem na hasło. Metoda brute-force z kolei polega na odgadywaniu hasła metodą próbowania wszystkich możliwych kombinacji znaków. Im dłuższe hasło i im bardziej kombinacja odbiega od normy, tym trudniejsze zadanie ma atakujący.

■ **PODSŁUCHANIE HASŁA**

Atakujący może zobaczyć nasze hasło, na przykład patrząc nam przez ramię, kiedy wpisujemy je na klawiaturze. Nasze hasło może również zostać podsłuchane za pomocą złośliwego oprogramowania, które rejestruje wszystko, co robimy na komputerze – łącznie ze zrzutami ekranu, nazwą używanych aplikacji i adresem WWW stron, które odwiedzamy. Jeszcze innym sposobem jest zastosowanie specjalnych aplikacji lub urządzeń, tak zwanych key-

PIN DO KARTY

Hasło nie zawsze musi być silne, jeśli system zabezpieczeń wyklucza możliwość jego złamania. Dobrym przykładem jest tutaj PIN do kart płatniczych, który składa się tylko z 4 cyfr. Złamanie tego hasła metodą brute-force (patrz tekst powyżej) przeciętnemu komputerowi zajęłoby mniej niż sekundę. Jednak wykorzystanie tej metody na przykład w bankomacie jest niemożliwe. Dlatego pozostaje jedynie odgadnięcie poprawnego PIN-u. Nie jest to łatwe, bo w tym przypadku mamy 10 tysięcy możliwych kombinacji i tylko trzy próby. Dlatego złodzieje kart płatniczych, zanim ukradną nam ten plastikowy środek płatniczy, najpierw próbują uzyskać nasz PIN, na przykład podglądając nas przy bankomanie lub w sklepie podczas dokonywania przez nas płatności albo stosując inne metody (ukryte czytniki w bankomatach, czy kamery skierowane na klawiaturę terminalu).

Więcej na: www.ebook4all.pl

loggerów, które zapisują wszystkie znaki wpisane na klawiaturze. Te metody najczęściej stosowane są na komputerach publicznych, na przykład w kawiarenkach internetowych. Niebezpieczeństwo wykradzenia hasła istnieje również, gdy do łączenia z internetem korzystamy z niezabezpieczonych sieci Wi-Fi.

WYŁUDZENIE HASŁA

Cyberprzestępcy do wyłudzenia naszego hasła stosują również wiele bardzo zuchwałych metod, doprowadzając do sytuacji, w której często ofiara sama zdradza swoje dane. Na przykład wysyłają e-mail z prośbą o podanie danych, bo na serwerze rzekomo była awaria i muszą uzupełnić na nim dane. Inną metodą jest na przykład e-mail z prośbą o potwierdzenie dużej wypłaty gotówki z naszego konta. Często z obawy o stratę znacznej kwoty, aby nie dopuścić do tej dziwnej transakcji, logujemy się na fałszywej stronie poprzez link wysłany w wiadomości. Choć witryna wygląda identycznie jak oryginalna strona banku, dane logowania trafiają do oszusta. Generalnie nie da się opisać, wszystkich dostępnych metod, których może użyć cyberprzestępca do wyłudzenia od nas hasła. Dlatego w tej kwestii musimy wykazać się dużą ostrożnością i podejrzliwością. Warto przede wszystkim stosować się do zasad zamieszczonych w powyższej ramce.

ZASADY BEZPIECZEŃSTWA

- nigdy nie zapisujmy swojego hasła w postaci jawnej (niezaszyfrowanej)
- nie należy przesyłać swojego hasła przez internet, na przykład za pomocą poczty e-mail w formie niezaszyfrowanej
- hasło do najważniejszych serwisów powinniśmy regularnie zmieniać co jakiś czas
- nie należy używać tego samego hasła do wielu różnych usług i serwisów
- nie należy wprowadzać swoich haseł podczas korzystania z niezaufanego komputera
- przed wprowadzeniem hasła należy dokładnie sprawdzić adres WWW oraz zabezpieczenia strony (dotyczy zwłaszcza bankowości internetowej)
- pamiętajmy, że żaden szanujący się serwis w internecie nie wysyła e-maili z prośbą o nasze hasło
- nikomu nie zdradzajmy swojego hasła

Tworzymy bezpieczne hasła

Wiemy już, jakie hasła są silne, oraz poznaliśmy ogólne reguły, które należy stosować podczas ich tworzenia, a także jakie hasła są łatwe do złamania. Wydawać by się mogło, że stworzenie bezpiecznego hasła to nic prostszego – wystarczy przecież wprowadzić długi ciąg znaków składający się z kombinacji liter (małych i wielkich), cyfr i symboli. Tylko czy takie hasło będzie wygodne? Nie, nie będziemy bowiem w stanie zapamiętać tego przypadkowego ciągu znaków. Jest jednak prosty sposób, aby tworzyć hasła, których układ poszczególnych znaków może wyglądać bardzo chaotycznie, ale dla właściciela jest on bardzo prosty do zapamiętania. Poznajmy go.

Hasło z ulubionej sentencji

Jedną z najłatwiejszych metod tworzenia bezpiecznych haseł jest wykorzystanie do tego celu znanej nam sentencji, na przykład cytatu z ulubionej książki czy też fragmentu piosenki.

1 Zaczynamy od zapisania zdania łatwego dla nas do zapamiętania, na przykład:

Wlazł kotek na płotek i mruga, piękna to piosenka, niedługa;

2 Teraz zamieniamy nasze zdanie na ciąg liter, na przykład używając pierwszych liter każdego słowa.

wknpimptpn

3 Następnie zwiększamy jego złożoność, na przykład zamieniając co drugą literę na dużą lub wszystkie litery z pierwszej połowy alfabetu.

WkNpImPtPn

4 Hasło dodatkowo komplikujemy, dodając do niego cyfry. Możemy na przykład zamienić niektóre litery na podobne do nich cyfry, na przykład **I** na **1**, a **W** na **3**.

3kNp1mPtPn

5 Dodatkowo zwiększamy długość poprzez znaki interpunkcyjne, które znajdują się w naszym zdaniu.

3kNp1m,PtP,n;

6 Dodajemy znaki specjalne, na przykład na początku i końcu hasła.

!3kNp1m,PtP,n;"

7 Bezpieczne hasło warto wprowadzić na klawiaturze kilkukrotnie, co ułatwi nam jego zapamiętanie.

8 Kolejne hasło możemy stworzyć, posługując się tym samym zdaniem, ale biorąc na przykład ostatnie litery każdego słowa. Pamiętajmy, aby unikać w haśle polskich znaków diakrytycznych, ponieważ nie w każdej sytuacji będziemy mogli je zastosować.

Menedżery haseł

Haseł nie powinniśmy zapisywać w postaci jawnej. Nie zawsze jednak jesteśmy w stanie zapamiętać wszystkich PIN-ów, loginów i haseł do wielu serwisów internetowych, szczególnie jeśli korzystamy z nich sporadycznie. Możemy je jednak przechowywać w sposób zaszyfrowany i zabezpieczony jednym silnym hasłem. Taką możliwość stwarzają nam aplikacje KeePass (rodzaj banku z zaszyfrowanymi danymi) oraz LastPass – wtyczka do przeglądarki, która zapamiętuje hasła do serwisów i loguje się do nich automatycznie. Zobaczmy, jak korzystać z tych narzędzi.

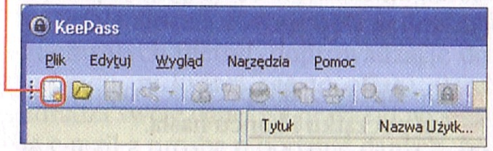
Korzystamy z KeePass

1 Z płyty dołączonej do Biblioteczki instalujemy najpierw aplikację KeePass (CD-KOD: 010), a następnie spolszczenie programu (CD-KOD: 011).

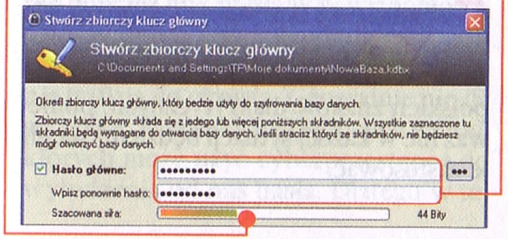
Więcej na: www.ebook4all.pl

2 Aby przełączyć program na język polski, klikamy w nim kolejno na menu View, Change Language... i dwukrotnie na Polish. Potwierdzamy zmiany kliknięciem na Tak.

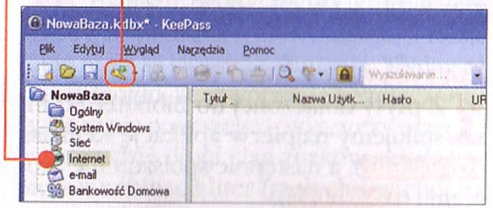
3 Zakładamy nową bazę z hasłami. W tym celu klikamy na ikonę ● i przycisk Zapisz.



4 W wyświetlonym oknie w pola ● wpisujemy główne hasło, które będzie chroniło wszystkie inne nasze hasła wprowadzone do programu. Musi ono więc być bezpieczne - jego siła szacowana jest na pasku ●. Klikamy na OK w tym i następnym oknie.

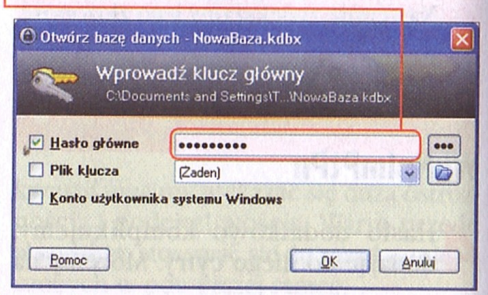


5 Zaznaczamy teraz grupę, w której chcemy wprowadzić nowy wpis, na przykład ● (domyślnie jest kilka podstawowych grup, możemy jednak tworzyć własne) i klikamy na ●.

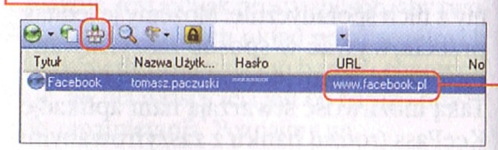


6 Uzupełniamy wszystkie pola ●, podając między innymi własne identyfikator i hasło, a następnie klikamy na OK.

7 Teraz, gdy będziemy chcieli przypomnieć sobie login i hasło, uruchamiamy KeePass i logujemy się do niego, wprowadzajac główne hasło ●. Następnie otwieramy odpowiedni wpis i po kliknięciu na ● ,zobaczymy podgląd hasła.



8 Z aplikacji KeePass możemy też otworzyć serwis i automatycznie zalogować się do niego na podstawie wprowadzonych danych. W tym celu dwukrotnie klikamy na adres URL w danym wpisie ● - zostanie otworzona strona serwisu w przeglądarce. Po kliknięciu na przycisk ● pola logowania zostaną automatycznie uzupełnione.

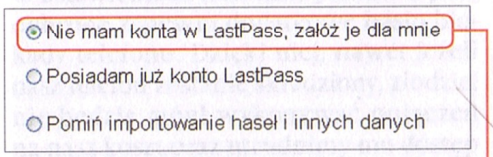


Wygodne logowanie z LastPass

Wszystkie przeglądarki oferują nam bardzo przydatną funkcję zapamiętywania danych logowania do serwisów internetowych, jak poczta e-mail, banki, sklepy internetowe. Jest to wygodne, bo nie wymaga od nas każdorazowego wpisywania tych danych, ma jednak olbrzymią wadę - jeśli ktokolwiek dostanie się do naszego komputera, ukradnie go lub włamie się przez internet, uzyska natychmiastowy dostęp do tych informacji bez konieczności wpisywania jakiegokolwiek hasła. Co gorsza, w większości wypadków przeglądarki przechowują te informacje, nie szyfrując ich!

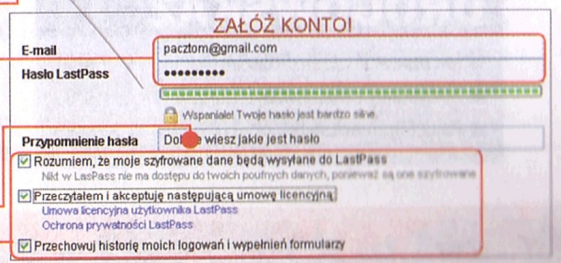
Jeśli zależy nam na wygodzie, lepiej skorzystać z programu LastPass, który będzie zapamiętywał nasze loginy i hasła wpisywane bezpośrednio w przeglądarkach. Ułatwi nam także logowanie do serwisów, wykorzystując w nich silne hasła, których nie musimy pamiętać. I to wszystko w maksymalnie bezpieczny sposób.

1 Z płyty dołączonej do Biblioteczki uruchamiamy instalację aplikacji LastPass (CD-KOD: 014).



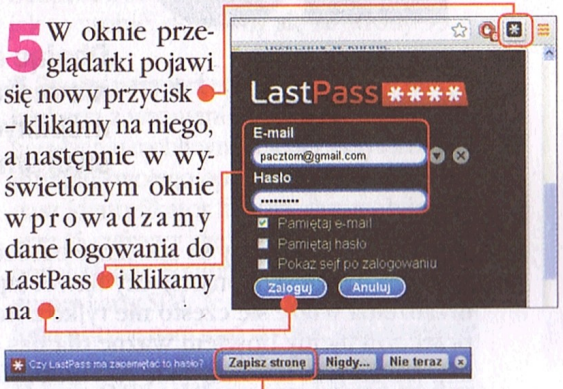
2 W trakcie instalacji wybieramy pozycję ● i klikamy na Następny.

3 Teraz zakładamy konto, wypełniając pola formularza. Wprowadzamy swój e-mail oraz główne hasło logowania ●, zdanie, które ułatwi nam przypomnienie sobie hasła ●, oraz zaznaczamy pozycje ●. Klikamy na Następny.

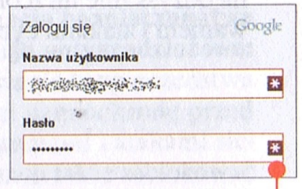


4 W kolejnym oknie ponownie wprowadzamy hasło LastPass i zatwierdzamy przyciskiem Save. Na koniec wystarczy kliknąć na przycisk Click to install LastPass, który widoczny będzie na nowo otworzonej witrynie domyślnej przeglądarki, w której zostanie dodana wtyczka LastPass.

5 W oknie przeglądarki pojawi się nowy przycisk ● - klikamy na niego, a następnie w wyświetlonym oknie wprowadzamy dane logowania do LastPass ● i klikamy na ●.



6 Od teraz za każdym razem podczas logowania się do nowych serwisów wtyczka LastPass będzie proponowała nam zapamiętanie danych - wystarczy kliknąć na przycisk ●, a potem na wyświetlonej stronie na Zapisz, aby w przyszłości formularz logowania został uzupełniony automatycznie przez LastPass ●.



Więcej na: www.ebook4all.pl

10 Smartfon i tablet

Dbając o bezpieczeństwo swoich danych, nie możemy zapominać o urządzeniach mobilnych. Dowiedzmy się, jak zabezpieczyć swój smartfon i tablet

Smartfony i tablety są znacznie bardziej narażone na zgubienie czy kradzież niż komputery stacjonarne czy nawet laptopy. Przykre zdarzenie związane z utratą urządzenia wiąże się często nie tylko z finansową szkodą. W smartfonach i tabletach przechowujemy bowiem ważne dla nas dane, nie tylko te o wartości sentymentalnej, jak zdjęcia czy filmy, ale również informacje, które w nieodpowiednich rękach mogą narazić nas na spore nieprzyjemności. Dlatego warto zadbać o ich odpowiednie zabezpieczenie. W tym rozdziale przeczytamy o tym, jak chronić swoje urządzenia mobilne, wykorzystując do tego celu mechanizmy systemowe, aplikacje producenckie i dodatkowe oprogramowanie. Z lektury dowiemy się również, jak zwiększyć szanse na odzyskanie utraconego sprzętu oraz jak ochronić się przed złośliwym oprogramowaniem i atakami cyberprzestępców.

tpa

DROGOWSKAZ

- Jak zapewnić bezpieczeństwo s. 91
- Korzystamy z wbudowanych funkcji s. 93
- Pakiet bezpieczeństwa od G Data s. 99

Jak zapewnić bezpieczeństwo

Aby chronić smartfon i tablet oraz zgromadzone na urządzeniach dane, powinniśmy stosować się do kilku podstawowych zasad. Poznajmy je oraz dowiedzmy się, jakie kroki należy poczynić, gdy nasze urządzenie zaginie.

■ **Bądź ostrożny i pilnuj swoich urządzeń:** Nowoczesny smartfon czy tablet to łakomy kąsek dla złodzieja. Dlatego zawsze powinniśmy przechowywać te urządzenia w bezpiecznym miejscu, na przykład w przedniej kieszeni spodni czy też wewnętrznej przegrodzie plecaka. Pozostawianie tych urządzeń na stoliku kawiarni czy też basenowej ławce to z pewnością nie jest dobry pomysł.

■ **Włącz blokadę:** Kod PIN to absolutne minimum w zakresie bezpieczeństwa telefonów komórkowych. Choć niektóre karty SIM (szczególnie usług pre-paid) mają domyślnie wyłączoną ochronę, warto ją uaktywnić (możemy to zrobić w ustawieniach telefonu). Jeszcze lepszą ochronę zapewni dodatkowe hasło blokady telefonu. Dzięki niej, nawet jeżeli nasz telefon zostanie skradziony, złodziej nie będzie mógł wykonywać połączeń na nasz koszt oraz utrudnimy mu dostęp do zawartości swojego urządzenia. Jak włączyć blokadę telefonu, dowiemy się ze strony 93.

■ **Wykonuj kopię danych:** W smartfonie przechowujemy wiele danych, których utrata często bywa bardziej dotkliwa niż samego urządzenia. Warto więc wykonywać regularną kopię tych danych, szczególnie że proces możemy przeprowadzać bezprzewodowo i zautomatyzować go – jak to zrobić, dowiemy się ze strony 95.

■ **Stwórz paszport urządzenia:** To nic innego jak karta z ważnymi informacjami o swoim urządzeniu mobilnym, między innymi numer infolinii swojego operatora komórkowego, nasz identyfikator klienta, numer telefonu oraz 15-cyfrowy identyfikator IMEI (International Mobile Equipment Identifier), a także numer karty SIM. Te dane w razie utraty telefonu ułatwią nam jego szybkie zablokowanie oraz zgłoszenie kradzieży na policji.
Numer IMEI telefonu znajdziemy na opakowaniu smartfona. Możemy też go w każdej chwili sprawdzić, wprowadzając na klawiaturze telefonu kod ***#06#**.

■ **Zainstaluj aplikację bezpieczeństwa i skonfiguruj funkcje antykradzieżowe:** Dobre oprogramowanie bezpieczeństwa mobilnego zapewni nam ochronę przed szkodliwymi programami i atakami sieciowymi. Pozwoli nam także zablokować dostęp do kontaktów, zdjęć i plików, uniemożliwiając złodziejom przejęcie naszych osobistych danych. Ponadto, tego typu aplikacje (a także rozwiązania systemowe i producenckie) pozwolą nam również zdalnie zlokalizować urządzenie. Odpowiednio konfigurując telefon, zostaniemy też poinformowani, jeśli zna-

Więcej na: www.ebook4all.pl

łazca naszego urządzenia wymieni w nim kartę SIM, wysyłając na wskazany numer wiadomość zawierającą nowy numer. Jak korzystać z tych narzędzi, dowiemy się ze stron 96–99.

■ **Zaszyfruj dane:** Przechowujmy poufne dane tylko w zaszyfrowanej postaci. Jeśli na swoim smartfonie musimy przechowywać ważne dane, na przykład identyfikatory i hasła do bankowości elektronicznej, wykorzystujmy do tego celu specjalne aplikacje, które szyfrują dane i pozwalają na dostęp do nich wyłącznie po podaniu hasła.
Jeżeli w naszym smartfonie bądź tablecie wykorzystujemy kartę pamięci do przechowywania danych, nie zapomnijmy także jej zaszyfrować. W innym wypadku złodziej będzie mógł ją w prosty sposób odczytać, korzystając ze zwykłego czytnika kart.

■ **Instaluj tylko z wiarygodnych źródeł:** Najlepiej aplikacje instalować wyłącznie z oficjalnych sklepów (przed publikacją są one sprawdzane, między innymi pod względem złośliwego kodu). Jeśli musimy zainstalować aplikację z innego źródła, warto najpierw uważnie je sprawdzić. Powinniśmy też sprawdzać wszystkie upoważnienia i regulaminy oraz zwracać szczególną uwagę na pozwolenia, o które proszą aplikacje podczas instalacji. Szczególnie dobrze zastanówmy się, zanim zainstalujemy programy domagające się pozwolenia na łączenie się z internetem, wysyłanie lub odbieranie SMS-ów, odbieranie połączeń telefonicznych lub otrzymanie dostępu do książki telefonicznej. Czy darmowa gra naprawdę potrzebuje tych wszystkich pozwoleń?

■ **Korzystaj z hotspotów Wi-Fi z głową:** Coraz więcej dostępnych jest publicznych punktów Wi-Fi. Zwykle są darmowe i oferują naprawdę szybkie połączenie. Niestety, łączenie z nimi zwykle nie jest szyfrowane, dlatego należy używać ich z rozwagą. Cyberprzestępcy tylko czekają, aż ktoś postanowi sprawdzić swój stan konta bankowego, zalogować się na poczcie czy przesłać do sieci poufne dane. Publicznych hotspotów lepiej nie używać do tego celu, a jeśli już musimy skorzystać na przykład z bankowości elektronicznej poza domem, znacznie bezpieczniej będzie odłączyć się od Wi-Fi i połączyć z internetem przez sieć komórkową.

■ **Bądź ostrożny w internecie:** Korzystając z internetu na smartfonie i tablecie, bądźmy ostrożni tak samo, jak w wypadku komputera – nie klikajmy na podejrzane linki oraz nie odpisujmy na maile z nieznanego źródła.

■ **Używaj tylko dedykowanych aplikacji:** Jeśli korzystamy z jakichś usług (na przykład bankowości elektronicznej czy też Facebooka) poprzez mobilne programy, używajmy tylko i wyłącznie do tego celu dedykowanych aplikacji przygotowanych przez swój bank lub producenta usługi, w których transmisja danych jest szyfrowana już na poziomie aplikacji.

■ **Aktualizuj oprogramowanie:** Należy regularnie uaktualniać system operacyjny i aplikacje, z których korzystamy. Producenci nie tylko dodają w nowych wersjach dodatkowe funkcje i poprawiają ich wygląd, ale przede wszystkim usuwają rozmaite błędy w systemie, zwiększając bezpieczeństwo urządzeń.

CO ZROBIĆ, GDY URZĄDZENIE NAM ZAGINIE

Stało się! Nie możemy znaleźć swojego smartfona. Gdzieś się zapodział albo po prostu został nam skradziony. Co powinniśmy zrobić? Oto cztery kroki, które w kolejności powinniśmy wykonać w wypadku zaginięcia telefonu.

KROK 1 – Zadzwoń na numer utraconego telefonu
Skorzystaj z innego telefonu, żeby zadzwonić do siebie. Być może po prostu go gdzieś zapodziałeś i w pobliżu usłyszysz znajomy dzwonek. Możesz też trafić na uczciwego znalazcę, który odbierze telefon i powie ci, gdzie możesz odebrać swoją własność.

■ **KROK 2 – Zlokalizuj swój smartfon**
Jeżeli masz oprogramowanie bezpieczeństwa lub włączyłeś odpowiednie funkcje systemowe, możesz zlokalizować swój smartfon, wysłać wiadomość na urządzenie i, w razie konieczności, zdalnie usunąć dane.

■ **KROK 3 – Zablokuj kartę SIM**
Jeśli jesteś pewien, że twój telefon naprawdę zniknął, powinieneś zablokować swoją kartę SIM, niezależnie od tego, czy masz abonament, czy telefon na kartę. Dzięki paszportowi swojego telefonu komórkowego będziesz miał wszystkie niezbędne dane do jego blokady.

■ **KROK 4 – Zgłoś incydent**
Jeżeli twój smartfon został skradziony na wakacjach, natychmiast zgłoś to lokalnej policji. W tym celu zabierz ze sobą paszport twojego telefonu komórkowego – dzięki niemu władze będą znały identyfikator IMEI. Jest to ważny dowód na wypadek późniejszego aresztowania złodzieja.

Korzystamy z wbudowanych funkcji

Obecnie każdy system mobilny oferuje wiele wbudowanych funkcji bezpieczeństwa, które pozwalają nam chronić zgromadzone na urządzeniu dane przed niepowołanymi osobami. Zobaczmy, jak je włączyć i z nich korzystać w dwóch najpopularniejszych systemach – Android (w Samsungu Galaxy S4) i iOS (iPhone 4).

Blokada ekranu

To najprostszy sposób zabezpieczenia smartfona. Do dyspozycji mamy kilka opcji, których dostępność zależy od modelu posiadanego smartfona:

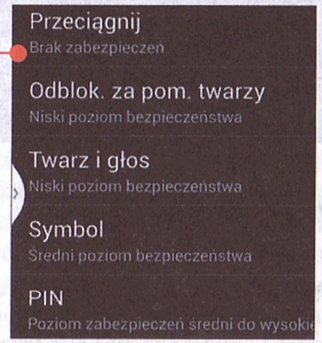
Przeciągnięcie – ta forma zabezpieczenia chroni jedynie przed przypadkowym wybudzeniem urządzenia (Android/iOS).
Wzór/Symbol – ekran zostanie odblokowany tylko po poprawnym narysowaniu wcześniej ustalonej ścieżki na ekranie składającym się z kilku pól (kropek). Jest to wygodne zabezpieczenie, ale łatwo da się obejść – wystarczy spojrzeć pod światło na ślady palca na wygaszonym ekranie (Android).
Kod PIN – skuteczna i dość wygodna metoda, umożliwia zabezpieczenie telefonu za pomocą czterocyfrowego kodu (Android/iOS).

Więcej na: www.ebook4all.pl

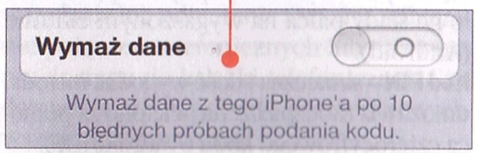
Hasło – najskuteczniejsza metoda, która pozwala zabezpieczyć smartfon dowolnym hasłem składającym się z liter i cyfr. (Android/iOS).

Face Unlock – ta opcja dostępna jest od czwartej wersji Androida i na wybranych modelach urządzeń z tym systemem. Do odblokowania służy nasza twarz, która wykrywana jest za pomocą obrazu z przedniej kamery. Choć teoretycznie metoda ta powinna być skuteczna, w rzeczywistości łatwo ją obejść, na przykład wykorzystując zdjęcie właściciela smartfona. Telefon może też odblokować osoba podobna do nas. Face Unlock nie jest też zbyt wygodny (Android).

■ **Android:** W urządzeniach z Androidem typ blokady konfigurujemy w ustawieniach na zakładce Ekran blokady.



■ **iOS:** W iPhonie i iPadzie rodzaj blokady wybieramy w ustawieniach na zakładce Ogólne. W systemie iOS dodatkowo możemy włączyć automatyczne wymazanie danych po 10 błędnych próbach podania kodu.



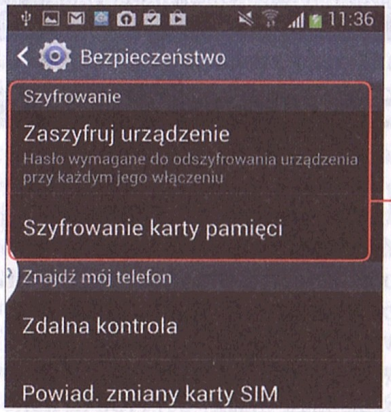
Szyfrowanie danych

Po zaszyfrowaniu pamięci smartfona, nikt, kto nie zna hasła blokady, nie będzie w stanie odczytać danych przechowywanych w urządzeniu.

■ **iOS:** Szyfrowanie w iPhonie i iPadzie jest bardzo ułatwione – włącza się automatycznie po aktywacji kodu blokady ekranu.

■ **Android:** W urządzeniach z systemem Android szyfrowanie pamięci włączamy manualnie. Proces trwa około godziny i przy każdym uruchomieniu zaszyfrowanego telefonu bądź tabletu trzeba wprowadzić hasło blokady, które musimy ustalić przed rozpoczęciem procesu szyfrowania. Musi się ono składać co najmniej z sześciu znaków i zawierać przynajmniej jedną cyfrę i literę.

Proces szyfrowania wymaga wcześniejszego naładowania baterii i do momentu jego ukończenia urządzenie powinno pozostać podłączone do ładowarki.



Jeśli w naszym smartfonie bądź tablecie używamy karty pamięci, możemy także włączyć jej szyfrowanie. Funkcje szyfrowania w systemie Android znajdziemy w ustawieniach na zakładce Bezpieczeństwo.

Backup danych

■ **iOS:** W urządzeniach z systemem iOS dostępna jest systemowa funkcja archiwizowania danych w chmurze Apple'a, czyli w iCloud. Dzięki usłudze możemy za pośrednictwem sieci Wi-Fi wykonywać codziennie kopie zapasowe ważnych danych, między innymi zdjęć i filmów z aparatu, danych aplikacji, ustawień urządzenia czy też wiadomości. W razie zgubienia lub kradzieży iPhone'a lub iPada można łatwo odzyskać te same informacje na nowym urządzeniu. Zobaczmy, jak włączyć archiwizację danych w iCloud.

1 W ustawieniach iPhone'a przechodzimy na zakładkę iCloud. Po naciśnięciu pola wprowadzamy swój identyfikator Apple ID oraz hasło.

2 Zaznaczamy, które elementy mają być synchronizowane z chmurą – pozwoli nam to uzyskać dostęp do niektórych danych na innych swoich urządzeniach oraz za pomocą strony **www.icloud.com**.

KOPIA NA DYSKU

Niezależnie od stosowanych usług do archiwizacji danych w chmurze zawsze warto wykonać dodatkowo tradycyjną kopię najważniejszych danych z urządzenia na dysk komputera.

3 Aby włączyć wykonywanie kopii bezpieczeństwa całej pamięci iPhone'a, w iCloud naciskamy pozycję Dysk i archiwum. Następnie za pomocą suwaka włączamy funkcję Archiwum iCloud. Od teraz archiwizacja danych iPhone'a będzie wykonywana automatycznie, gdy urządzenie będzie znajdowało się w zasięgu sieci Wi-Fi i podłączone zostanie do ładowarki. W każdej chwili możemy też wykonać archiwizację ręcznie, naciskając przycisk Archiwizuj teraz.

4 Aby odtworzyć nowe urządzenie z archiwum iCloud, na ekranie wybieramy opcję, a następnie wprowadzamy nazwę swojego konta i hasło usługi iCloud. Z listy dostępnych archiwów wybieramy to, które chcemy odtworzyć. Jeśli chcemy przywrócić dane na używanym urządzeniu, najpierw wymazujemy jego zawartość.

Więcej na: www.ebook4all.pl

Android: System Google nie ma systemowego backupu, który zapewni nam kompleksową archiwizację wszystkich danych. Kontakty, ustawienia i dane aplikacji są domyślnie synchronizowane z kontem Google i w każdej chwili możemy je przywrócić. Niestety, konto Google nie daje możliwości bezpośredniego zapisania muzyki i filmów – do tego celu możemy jednak wykorzystać pośrednio usługę Google+. Dzięki niej zdjęcia i filmy będą zapisywane w internecie w prywatnym albumie serwisu Google+.

1 Aby włączyć automatyczne przesyłanie zdjęć i filmów, uruchamiamy aplikację Google+ (jeśli nie mamy jej na swoim urządzeniu, instalujemy ją z Google Play). Po zalogowaniu się (identyfikatorem konta Google) wyświetli się ekran, na którym konfigurujemy sposób automatycznej kopii zapasowej pamięci aparatu, na przykład w sposób.

2 Po zatwierdzeniu przyciskiem Gotowe nasze zdjęcia będą automatycznie archiwizowane w Google+.

Funkcje lokalizacyjne

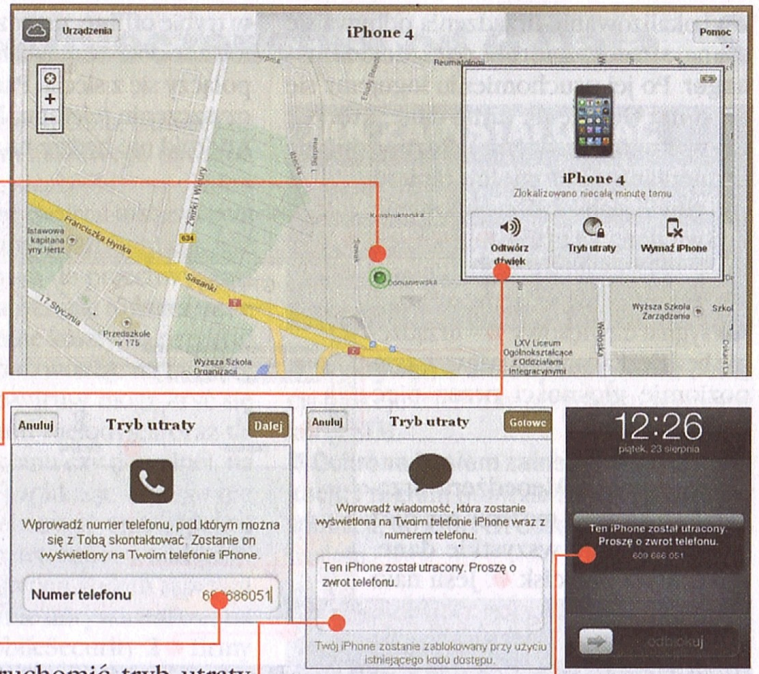
Zarówno w systemie Android, jak i iOS dostępne są systemowe funkcje zdalnej lokalizacji urządzeń. Dzięki nim zgubiony smartfon czy tablet możemy łatwo odnaleźć na cyfrowej mapie za pomocą dowolnej przeglądarki internetowej. Pamiętajmy jednak, że w naszym urządzeniu muszą być włączone funkcje lokalizacji (między innymi włączony odbiornik GPS), a także uruchomiona transmisja danych. Zobaczmy, jak skonfigurować urządzenia, aby w razie jego zgubienia lub kradzieży poznać jego lokalizację.

iOS: Usługa Znajdź mój iPhone to jedna z funkcji iCloud – jak ją uruchomić, dowiedzieliśmy się na stronie 95. Aby możliwe było skorzystanie ze zdalnej funkcji lokalizacji, wystarczy w ustawieniach na zakładce iCloud włączyć Znajdź iPhone.

1 Aby zlokalizować urządzenie, uruchamiamy stronę **www.icloud.com/find**. Na otworzonej witrynie wprowadzamy swój identyfikator Apple ID oraz hasło (te same dane, z których korzystamy w urządzeniu) i klikamy na.

2 Po chwili zostanie wyświetlona mapa, a na niej oznaczony punkt lokalizacji naszego urządzenia.

3 Usługa Znajdź mój iPhone umożliwia dodatkowo odtworzenie dźwięku na urządzeniu z maksymalną głośnością (przycisk) – ułatwia znalezienie zapodzianego w pobliżu smartfona, który jest wyciszony.

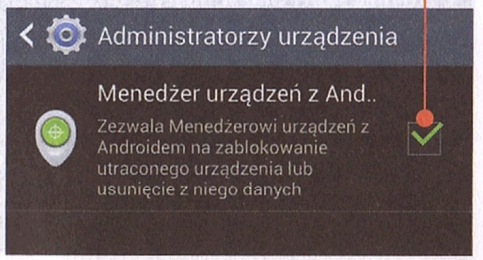


4 Możemy też uruchomić tryb utraty urządzenia – przycisk Tryb utraty. W kolejno wyświetlanych oknach możemy wprowadzić informacje dla znalazcy – numer kontaktowy do siebie oraz wiadomość, która zostanie wyświetlona na ekranie urządzenia.

5 Ostatnią deską ratunku jest zdalne wymazanie danych w urządzeniu. Po kliknięciu na przycisk Wymaż iPhone – wszystkie dane zostaną usunięte z pamięci iPhone'a lub iPada.

Android: Systemowa funkcja lokalizacji i zdalnego usunięcia danych (menedżer urządzeń) w smartfonach i tabletach z Androidem została wprowadzona przez Google dość niedawno. Dlatego o możliwości skorzystania z niej na razie wie niewielu użytkowników.

1 Skorzystanie z niej nie wymaga instalowania dodatkowych aplikacji czy specjalnej konfiguracji. W niektórych urządzeniach musimy jedynie uaktywnić Menedżera urządzeń jako administratora, aby możliwe było zdalne zablokowanie urządzenia i wymazanie z niego danych. W tym celu w ustawieniach systemu na zakładce Bezpieczeństwo naciskamy Administratorzy urządzenia i zaznaczamy pozycję.

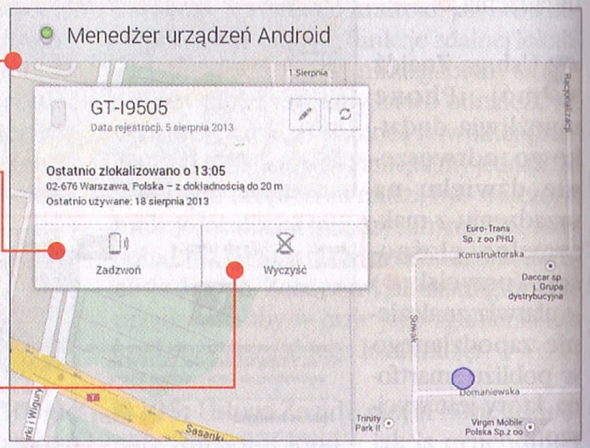


Więcej na: www.ebook4all.pl

2 Lokalizowanie urządzenia odbywa się na stronie **android.com/devicemanager**. Po jej uruchomieniu logujemy się do konta Google (te same dane, których używamy w urządzeniu). Rozpocznie się namierzanie telefonu lub tabletu i po chwili jego lokalizacja zostanie wyświetlona na mapie.

3 W programie możemy włączyć sygnał dźwiękowy – urządzenie będzie dzwonić na najwyższym poziomie głośności przez pięć minut.

4 Za pomocą Menedżera urządzeń Android możemy również zdalnie usunąć wszystkie dane, klikając na przycisk. Jeśli nasz smartfon bądź tablet jest aktualnie w trybie offline, urządzenie zostanie zresetowane do ustawień fabrycznych, gdy tylko połączy się z siecią. Pamiętajmy, że po wyczyszczeniu telefonu, Menedżer urządzeń Android nie będzie na nim działał.



BEZPIECZEŃSTWO OD PRODUCENTA

Niemal każdy producent urządzeń z Androidem oferuje własne rozwiązania bezpieczeństwa. Na przykład w smartfonach i tabletach Samsunga po założeniu specjalnego konta możemy skorzystać z podobnych do systemowych rozwiązań bezpieczeństwa – zdalnego zarządzania, lokalizacji czy kopii zapasowych wybranych danych i ustawień. Przydatną funkcją w smartfonach tego koreańskiego producenta jest powiadamianie o zmianie karty SIM w naszym urządzeniu. Po odpowiednim skonfigurowaniu usługi w momencie podmiany SIM-a zostanie wysłany z niego SMS na wskazany przez nas numer dodatkowy (na przykład bliskiej nam osoby). Numer nowej podmienionej karty SIM z pewnością okaże się przydatny przy zgłoszeniu kradzieży na Policji.

Usługa Find my mobile firmy Samsung oferuje bardzo wiele funkcji, między innymi śledzenie urządzenia, a także możliwość jego zdalnego blokowania, przekazywanie połączeń i wiadomości oraz wyczyszczenie pamięci urządzenia

Pakiet bezpieczeństwa od G Data

Smartfony i tablety są coraz bardziej zagrożone atakiem złośliwego oprogramowania. Wirusów, szczególnie na platformę Android, przybywa w zastraszającym tempie. Zainfekowany smartfon może być wykorzystany nie tylko do przechwycenia naszych poufnych danych, ale również może narazić nas na ogromne koszty, na przykład wysyłając SMS-y lub dzwoniąc na numery Premium. Aplikacje-wirusy mogą kryć się pod grami, pakietami melodyjek oraz tapet i wygaszaczy ekranu czy dowolnej, na pozór wartościowej aplikacji. Dlatego nie powinniśmy bagatelizować tego aspektu bezpieczeństwa smartfonów i tabletów. Ochronę przed złośliwym kodem zapewni nam oprogramowanie antywirusowe, na przykład pakiet MobileSecurity 2 firmy G Data, który dla Czytelników dostępny jest w atrakcyjnej cenie.

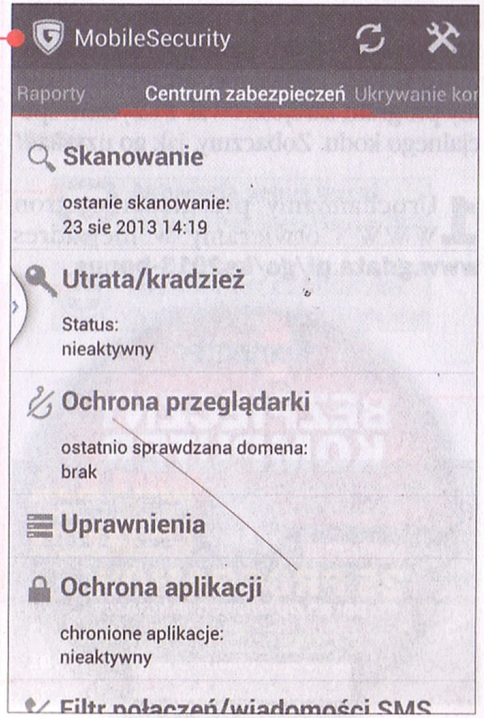
JAK ZAINSTALOWAĆ

Informacje, jak pobrać i zainstalować MobileSecurity 2 uzyskamy z e-maila, który otrzymamy od firmy G Data po zarejestrowaniu pakietu IS 2014 zgodnie z opisem na stronach 100–101.

Co oferuje pakiet od G Data

MobileSecurity 2 to kompleksowa ochrona naszego smartfona lub innego urządzenia z systemem Android. Skutecznie chroni naszą tożsamość oraz poufne dane przechowywane w telefonie lub tablecie przed wirusami i programami szpiegującymi. Zobaczmy, jakie funkcje oferuje.

- **Ochrona podczas surfowania:** Aplikacja chroni przed próbą phishingu podczas surfowania.
- **Zabezpieczenie przed niebezpiecznymi programami:** Menedżer aplikacji sprawdza uprawnienia zainstalowanych programów.
- **Ochrona przed kradzieżą:** Możliwość odczytania lokalizacji telefonu oraz zdalne usunięcie danych zapisanych na urządzeniu.
- **Wykrywanie zmiany karty SIM:** Funkcja blokuje telefon w przypadku wymiany karty SIM.
- **Ochrona hasłem zainstalowanych aplikacji:** Program pozwala na tworzenie listy aplikacji, do których dostęp chroniony jest hasłem.



Więcej na: www.ebook4all.pl

PAKIET G DATA IS 2014

Czytelnicy książki mogą za darmo przez 90 dni korzystać z pakietu bezpieczeństwa G Data InternetSecurity 2014. Dowiedzmy się, jak go zainstalować i uzyskać kod rejestracyjny

Pakiet bezpieczeństwa G Data IS 2014 zawiera takie moduły, jak: antywirus, firewall, antyspam, kontrola rodzicielska, niszczarka plików i menedżer autostartu. Oferowane funkcje zapewniają bardzo wysoki poziom bezpieczeństwa dla naszego systemu operacyjnego. Czytelnicy książki mogą z tego zestawu narzędzi korzystać za darmo przez 90 dni, a później mogą nabyć przedłużenie licencji w atrakcyjnej cenie promocyjnej.

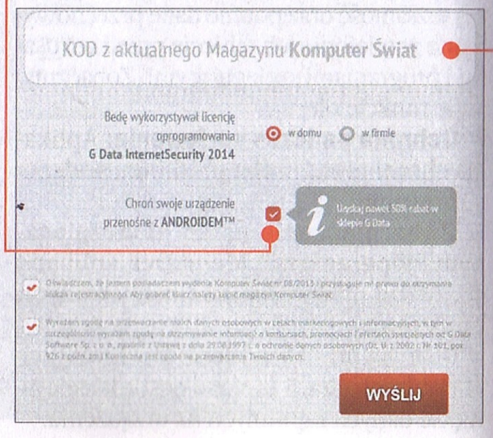
Jak uzyskać kod rejestracyjny

Aby uzyskać 90 dni pełnej ochrony za pomocą G Data InternetSecurity 2014, musimy program zarejestrować z użyciem specjalnego kodu. Zobaczmy, jak go uzyskać.

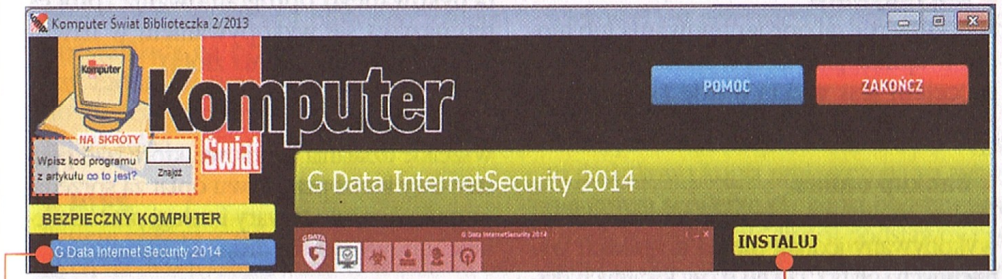
1 Uruchamiamy przeglądarkę stron WWW i otwieramy w niej adres **www.gdata.pl/go/ks2013-bonus**.

2 Wypełniamy formularz rejestracyjny, wpisując odpowiednie dane w wyświetlone pola. Kod widoczny na nadruku płyty Biblioteczki wprowadzamy w pole . Musimy pamiętać, aby podać własny, działający adres e-mail. Zaznaczamy także wszystkie niezbędne opcje (jeśli dodatkowo chcemy z rabatem nabyć program G Data MobileSecurity 2 (opisany na stronach 90–99), zaznaczamy), po czym klikamy na przycisk WYŚLIJ. (**Uwaga!** Formularz może się nieco różnić od zaprezentowanego poniżej).

3 Na podany w formularzu adres otrzymamy wiadomość e-mail zawierającą link aktywacyjny. Klikamy na niego – dzięki temu po chwili otrzymamy drugą wiadomość, a w niej kod do pełnej wersji pakietu G Data InternetSecurity 2014 oraz dokładną instrukcję rejestracji.



DLA CZYTELNIKÓW



Instalacja pakietu

1 Do napędu wkładamy płytę Biblioteczki i czekamy na uruchomienie głównego menu. Po jego starcie klikamy na , a potem na , uruchamiając instalator.

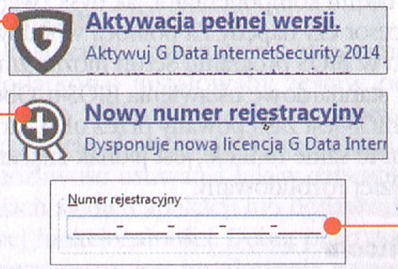
2 Gdy pojawi się systemowe ostrzeżenie o zabezpieczeniach, klikamy w jego oknie na Uruchom. Po chwili pojawi się okno instalatora pakietu.

3 Przechodzimy przez kolejne okna instalatora, klikając na przycisk Dalej >. Kolejno: akceptujemy warunki licencji, możemy przystąpić do inicjatywy G Data Malware Information, umożliwiającej przekazywanie informacji o wykrytych szkodnikach do laboratoriów G Data, i wybieramy dodatkowe moduły, które zostaną zainstalowane razem z pakietem. Na koniec klikamy na Instaluj.

4 Ponieważ w poradzie z poprzedniej strony uzyskaliśmy numer rejestracyjny, to w kolejnym oknie instalatora klikamy na pozycję , a potem na .

5 W pole wpisujemy nasz indywidualny kod rejestracyjny (nie kod bonusowy Komputer Świata, tylko ten przesłany nam e-mailem przez firmę G Data). Uzupełniamy także wszystkie pola formularza oznaczone symbolem gwiazdki. Klikamy na Zarejestruj.

6 Instalację kończymy, klikając na Zakończ. Komputer uruchomi się ponownie z oprogramowaniem G Data InternetSecurity 2014 działającym w pełnej wersji.



DLA FIRM

Czytelnicy otrzymują licencję do użytku domowego. W wypadku chęci korzystania z pakietu w firmie musimy dokupić rozszerzenie licencji. Informacje, jak to zrobić, znajdziemy w e-mailu rejestracyjnym.

Więcej na: www.ebook4all.pl

TRUDNE POJĘCIA I TERMINY

Antyspyware
Specjalny rodzaj oprogramowania lub moduł w aplikacjach bezpieczeństwa, którego celem jest wykrywanie i eliminacja z dysku programów szpiegujących.

Backup online
Proces tworzenia kopii zapasowej plików wykonywany jednak nie na nośnikach wymiennych (płyty CD/DVD) czy lokalnych dyskach twardych. W wypadku backupu online dane są kopiowane na zewnętrzne serwery w internecie – pliki są więc zabezpieczone niezależnie od zdarzeń, które mogą dotknąć nasze lokalne urządzenia i nośniki.

BIOS
Program zapisany w specjalnym układzie na płycie głównej. BIOS testuje sprzęt po włączeniu komputera, uruchamia system operacyjny, kontroluje transfer danych pomiędzy takimi komponentami, jak dysk twardy, procesor czy napędy. Za pomocą wbudowanego w BIOS programu Setup można zmieniać standardowe ustawienia BIOS-u. Obecnie BIOS jest zastępowany przez uEFI, który pełni te same funkcje, jest jednak znacznie bardziej rozbudowany.

Bitcoin
Cyfrowa waluta zaprojektowana w 2009 roku. W założeniu odporna na działania wszelkich banków centralnych (nie jest możliwe odgórne sterowanie jej wartością) oraz bezpieczna dzięki rozproszonej sieci serwerów przechowujących dane transakcji. Bitcoiny można kupować w specjalnych serwisach internetowych lub samodzielnie generować za pomocą dedykowanego oprogramowania (proces ten nazywa się wykopywaniem w nawiązaniu do wydobywania złota).

E-commerce
Wszelkie działania handlowe, które jako podstawowy kanał przepływu opłat za sprzedawane/kupowane towary i usługi oraz zawierane umowy stosują drogę elektroniczną.

EICAR
Europejski Instytut Badań Wirusów Komputerowych – organizacja, która koncentruje się na szukaniu metod zwiększania skuteczności oprogramowania antywirusowego oraz przeciwdziałaniu rozprzestrzeniania malware'u.

Hotspot
Otwarty, dostępny dla każdego punkt dostępowy sieci bezprzewodowej. Hotspoty działają w hotelach, restauracjach, dworcach, lotniskach, centrach handlowych czy na ulicach miast.

Kompresja
Proces redukcji miejsca, które zajmują dane komputerowe. Bezstratna kompresja to taka, gdzie rozpakowane dane są identyczne z oryginalnymi (na przykład ZIP, RAR), stratna zaś to taka, przy zastosowaniu której następuje utrata części danych oryginalnego pliku (na przykład MP3 czy kompresja wideo DivX).

Malware
Zbiorczy termin określający oprogramowanie niebezpieczne dla systemu operacyjnego i zgromadzonych w komputerze danych. Malware'em mogą być wirusy czy konie trojańskie.

NFC
Standard komunikacji bliskiego zasięgu pozwalający na przesyłanie danych między zgodnymi urządzeniami na odległość do 20 centymetrów. Ang. *Near Field Communication*.

NTFS
System plików (czyli sposób organizacji danych na dysku) stosowany w Windows od Windows 2000. Pozwala w dużym stopniu zarządzać uprawnieniami i przydziałami, co sprawia, że jest bardzo bezpieczny.

Obraz partycji
Specjalny plik tworzony przez program do backupu danych, który zawiera nie tylko wszystkie pliki zapisane na wybranej partycji, ale także ich logiczną strukturę. Po przywróceniu obrazu odzyskujemy dokładny stan systemu lub partycji z chwili wykonania obrazu.

Ochrona rezydentna
Moduł w oprogramowaniu zabezpieczającym, który nieustannie w tle monitoruje uruchomione aplikacje i wykonywane operacje, szukając podejrzanych aktywności, które mogą być efektem działań szkodników.

PayPal
Usługa płatności internetowych. Wystarczy znać adres e-mail użytkownika PayPala, aby móc przesłać do niego pieniądze.

PEGI
Ogólnoeuropejski System Klasyfikacji Gier – jego celem jest kontrola gier pod względem zawartych treści i przyznawanie stosownych ograniczeń wiekowych dla konkretnych tytułów. Dzięki PEGI, kupując grę, z jej opakowania możemy dowiedzieć się, dla jakiej grupy wiekowej jest przeznaczona oraz jakie treści potencjalnie szkodliwe zawiera.

Redundancja
W wypadku backupu, redundantna kopia to dodatkowa kopia umieszczona na zupełnie innym serwerze niż kopia podstawowa. Dzięki temu w razie awarii podstawowego serwera dostępny jest backup z drugiego.

Skrócony link
Długi adres internetowy witryny lub innej treści w sieci zamieniony na niepowtarzalny krótki adres łatwy do przekazania innym internautom, ale niewskazujący bezpośrednio na treść. Usługa oferowana przez wiele serwisów, w tym Google (pod adresem goo.gl). Prawdziwy adres odszyfrujemy dzięki witrynie **www.trueurl.net**. Ang. *short URL*.

Update
Aktualizacja – nowa wersja programu lub dodatkowo instalowany zestaw poprawek do aplikacji lub systemu operacyjnego. Dzięki aktualizacjom producenci mają możliwość usuwania luk w zabezpieczeniach swoich aplikacji lub dodawania nowej funkcjonalności. Dobrą praktyką bezpieczeństwa jest instalowanie wszystkich dostępnych update'ów do Windows i używanych przez nas programów.

Wirtualna karta kredytowa
Karta, która istnieje tylko w systemie elektronicznym banku. Z jej numeru, podobnie jak kodu CVV, możemy korzystać tylko do rozliczeń drogą elektroniczną.

Więcej na: www.ebook4all.pl

Biblioteczka Komputer Świat

AUTORZY: Paweł Gajewski, Rafał Kamiński, Mariusz Michalski, Tomasz Paczuski, Arkadiusz Świostek, Karol Żebruń

REDAKTOR PROWADZĄCY: Paweł Paczuski

PRZYGOTOWANIE PŁYTY CD: Mariusz Michalski

PROJEKT OKŁADKI: Robert Dobrzyński

DZIAŁ DTP: Robert Dobrzyński, Mariusz Rybak

KOREKTA: Jolanta Rososińska

ISBN: 978-83-7813-461-9
Warszawa 2013

© Copyright by Ringier Axel Springer Polska Sp. z o.o.

Wydawca: RINGIER AXEL SPRINGER POLSKA Sp. z o.o.,
02-672 Warszawa, ul. Domaniewska 52
tel. 22 2320000, 22 2320001
www.ringieraxelspringer.pl

ringier axel springer

DYREKTOR WYDAWNICZY: Paweł Paczuski

MENEDŻER DS. WYDAWNICZYCH: Paweł Bulwan

PROMOCJA: Michał Bajerski tel. 22 2320055

DRUK I OPRAWA: DRUK-INTRO S.A., Inowrocław

EGZEMPLARZE ARCHIWALNE:
tel. 22 7613214
infolinia 801 000869
e-mail: prenumerata.axel@infor.pl (zamówienia),
kontakt.axel@infor.pl (pytania i reklamacje)

SPRZEDAŻ INTERNETOWA: kiosk.literia.pl

KONTAKT Z REDAKCJĄ:
TEL: 22 2320078 (w godzinach 10–17)

INTERNET: www.komputerswiat.pl

E-MAIL: biblioteczka@komputerswiat.pl

Teraz kupisz
w dziale prenumeraty
tel. 22 7613214
oraz w aplikacji KŚ+
(www.ksplus.komputerswiat.pl)

KOMPUTER ŚWIAT BIBLIOTECZKA

Biblioteczka

Komputer Świat

KOMPLETNA OCHRONA

O bezpieczeństwie komputera pisze się dużo, ale najczęściej wyrywkowo. I tak samo chronimy nasze dane: wiemy, jak zabezpieczyć pecet przed wirusami, ale umknie nam phishing czy spyware. Pora z tym skończyć. Ta książka to kompendium wiedzy o wszystkich zagrożeniach informatycznych, które domowy użytkownik komputera powinien znać i wiedzieć, jak się chronić.

Każdy rozdział zawiera zarówno sporą dawkę przydatnej wiedzy teoretycznej, jak i praktyczne, opisane krok po kroku wskazówki, których cel jest jasny: zbudowanie w pececie ochrony skrojonej na miarę. Takiej, która nie spowalnia komputera i nie jest uciążliwa w codziennym użytkowaniu, a jednocześnie zapewnia wysoki poziom bezpieczeństwa przed szkodnikami i innymi zagrożeniami, które mogą wziąć na celownik dysk naszego komputera.

CENA 13,90 zł
w tym 5% VAT

KOMPUTER
ŚWIAT
BIBLIOTECZKA